Escola de Ciências Sociais e Humanas

Departamento de Economia Política

Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas

Pedro Carvalhais de Abreu Matos

Dissertação submetida como requisito parcial para obtenção do grau de Mestre em Economia e Políticas Públicas

Orientadora:
Professora Doutora Isabel Salavisa Lança, Professora Associada (com Agregação)

ISCTE – Instituto Universitário de Lisboa

Outubro, 2018

AGRADECIMENTOS

A concretização deste desafio só foi possível com a colaboração, direta e indireta, de muitas pessoas. A elas lhes devo um agradecimento.

Em primeiro lugar, a todos aqueles que, ao longo de alguns anos, contribuíram para aguçar a minha curiosidade e o gosto pelo tema que me propus estudar. Os textos que produziram, as conversas e as discussões que tivemos foram importantes contributos para a consolidação de conhecimentos e o despertar para uma contínua necessidade de aprender sempre mais.

Igualmente importante foi o saber transmitido por todo o corpo docente do Mestrado em Economia e Políticas Públicas que ajudou a solidificar as bases deste exercício final de curso.

Aos que aceitaram participar naquilo a que aqui chamei de “entrevistas” mas que, na verdade, se revelaram momentos de partilha de conhecimento e nos quais aprendi bastante. A eles, que por via do compromisso assumido não os poderei enunciar, o meu muito obrigado.

À Professora Doutora Isabel Salavisa pela sábia orientação e, acima de tudo, pelas assertivas chamadas de atenção ao longo deste processo de investigação.

Finalmente, e porque a elas devo muito pelo apoio e compreensão, às duas pessoas que sistematicamente se viram privadas da minha presença e participação no seio familiar em resultado dos esforços que coloquei nesta tarefa académica. Sem a Ana e a Beatriz a conclusão deste projeto não teria sido possível.

RESUMO

A história mostra que as revoluções industriais introduziram alterações profundas a todos os níveis: social, económico e político. Concomitantemente, a globalização potencia processos de transformação digital tornando pessoas e organizações cada vez mais dependentes das TIC, em especial do Ciberespaço e da Internet.

Verifica-se um aumento na implementação de políticas públicas, nacionais e europeias, que visam incentivar a transformação digital das economias, destacando os seus benefícios económicos, independentemente da dificuldade verificada na medição do seu impacto nos PIB nacionais e globais. Mas se se aceita que estes processos podem acrescentar benefícios às empresas e à economia em geral, eles podem também revelar riscos muitas vezes ignorados.

Iniciámos o nosso estudo tentando perceber a ação das empresas, em especial das PME, face ao risco de segurança digital, mas depressa nos vimos confrontados com a inexistência de dados que nos pudessem orientar no desenho de um panorama nacional. Na análise do quadro de políticas públicas, nacional e europeu, para identificar instrumentos ao dispor das organizações para lidar com os riscos de cibersegurança, percecionámos que a adoção pelas organizações, em Portugal, de culturas de cibersegurança ainda é incipiente.

Considerando que em matéria de cibersegurança parece existir alguma insatisfação com a ação do Estado, o nosso trabalho tenta consolidar um conjunto de relações das organizações com a transformação digital e o risco de segurança digital, sintetiza práticas passiveis de serem adotadas pelas organizações, e apresenta ainda uma proposta sobre o papel do Estado em matéria de políticas públicas na área da cibersegurança em Portugal.

Palavras-chave: Cibersegurança, Transformação Digital, PME, Políticas Públicas

Classificação JEL: M15, O38

ABSTRACT

History shows that industrial revolutions brought about deep shifts at all levels: social, economic and political. At the same time, globalisation fosters digital transformation processes, making people and organisations increasingly dependent on ICT, especially of the cyberspace and the Internet.

There is an increase implementation of public policies, both national and European, aimed at stimulating the digital transformation of economies by arguing their economic benefits, regardless of the difficulty in measuring its impact on national and global GDP. However, if one considers that these processes can generate benefits to companies and the economy in general, they may also cause risks that are often ignored.

We started our study trying to perceive the action of companies, especially SMEs, in the face of the risk of digital security, but we were soon confronted with the lack of data that could guide us in the design of a national framework. In analysing the national and European public policy framework to identify instruments available to organisations to deal with cybersecurity risks, we realized that the adoption of cybersecurity cultures by organisations in Portugal is still incipient.

Considering that there seems to be some dissatisfaction with the action of the State in cybersecurity, our work tries to consolidate a set of relationships between organizations with digital transformation and digital security risks, synthesizes practices that can be adopted by organisations, and submits a proposal on the role of the State regarding cybersecurity public policies in Portugal.

Keywords: Cybersecurity, Digital Transformation, SME, Public Policies

JEL Classification System: M15, O38

ÍNDICE

ÍNDICE DE QUADROS

ÍNDICE DE FIGURAS

GLOSSÁRIO DE SIGLAS

AP2SI	-	Associação Portuguesa para a Promoção da Segurança da Informação
APDC	-	Associação Portuguesa para o Desenvolvimento das Comunicações
APDSI	-	Associação para a Promoção e Desenvolvimento da Sociedade de Informação
AR	-	Assembleia da República
CACDLG	-	Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias
CNCS	-	Centro Nacional de Cibersegurança
CNPD	-	Comissão Nacional de Proteção de Dados
CSC	-	Cultura de Cibersegurança
CSSC	-	Conselho Superior de Segurança do Ciberespaço
ENISA	-	European Union Agency For Network and Information Security
ENSC	-	Estratégia Nacional de Segurança do Ciberespaço
FCT	-	Fundação para a Ciência e a Tecnologia, IP
FMI	-	Fundo Monetário Internacional
GNS	-	Gabinete Nacional de Segurança
I&D	-	Investigação e Desenvolvimento
IDC	-	International Data Corporation
INE	-	Instituto Nacional de Estatística
IoT	-	Internet das Coisas
ISO	-	International Organisation for Standardisation
JOUE	-	Jornal Oficial da União Europeia
MSI	-	Missão para a Sociedade da Informação
OCDE	-	Organização para a Cooperação e Desenvolvimento Económico
ONU	-	Organização das Nações Unidas
PIB	-	Produto Interno Bruto
PME	-	Pequenas e Médias Empresas
RA	-	Regiões Autónomas
RAA	-	Região Autónoma dos Açores
RAM	-	Região Autónoma da Madeira
RGPD	-	Regulamento Geral sobre a Proteção de Dados
SIS	-	Serviço de Informações de Segurança
TIC	-	Tecnologias de Informação e Comunicação
UE	-	União Europeia
UMIC	-	Agência para a Sociedade do Conhecimento, IP
UNCTAD	-	United Nations Conference on Trade and Development
WEF	-	World Economic Forum

INTRODUÇÃO

No contexto da atual revolução industrial, tem vindo a assistir-se a uma transformação da sociedade através da adoção das Tecnologias de Informação e Comunicação (TIC) num ritmo acelerado e com efeitos disruptivos em todos as áreas: social, económica e política. A investigação e o desenvolvimento científico e tecnológico têm potenciado o aparecimento de novos instrumentos e meios de desmaterialização de processos, produtos e serviços, sendo a adoção das TIC pelos diversos agentes muito impulsionada por incentivos diretos e indiretos.

Muito por causa do efeito da globalização, as várias medidas de estímulo ao desenvolvimento das economias encontram agora espelho a nível internacional, pelo que em Portugal, e em especial nas organizações, a transformação digital pode ser observada não só como uma resposta às medidas do quadro nacional, mas também àquelas que têm origem na União Europeia. Verifica-se, portanto, uma crescente aposta pelos agentes económicos, pelos Estados e pelas Organizações Internacionais no aprofundamento da economia digital, por se acreditar que poderá ser um motor de desenvolvimento e crescimento económico e social, independentemente da dificuldade verificada na sua avaliação em termos do seu peso nas economias nacionais.

Mas se se encontram potenciais vantagens na transformação digital das organizações, em particular das empresas, os potenciais riscos associados não devem ser ignorados. A transferência da atividade das organizações para os ambientes digitais, que passam a estar interligadas ou mais facilmente acessíveis dada a natureza da Internet e do ciberespaço, comporta alguns riscos que são, muitas vezes, descurados no momento da opção pela transformação digital ou relegados para fases posteriores desse processo.

Os relatos e evidências de ocorrência de incidentes, e também a escala destes, têm vindo a aumentar ao longo dos anos indiciando a existência de perdas e prejuízos avultados para as empresas, com um sério impacto na sua atividade, e onde, grande parte das vezes, também os cidadãos e os Estados são afetados. Hoje em dia, o acesso facilitado à tecnologia coloca os agentes económicos em situações de maior vulnerabilidade dado que esta passou a estar acessível a um conjunto mais vasto de atores com intenções duvidosas e/ou ilegítimas. Mas o mesmo acesso à tecnologia também está facilitado aos agentes económicos para que a possam colocar à disposição da sua própria proteção.

A ação das organizações em relação à sua proteção em ambientes digitais, isto é, à implementação de uma cultura de cibersegurança, pode ser condicionada, positiva ou negativamente, por diversos fatores internos e externos: o conhecimento e a sensibilidade para o tema, os recursos financeiros, os meios técnicos e humanos disponíveis, e ainda os estímulos e incentivos, entre outros.

No meio envolvente à cibersegurança – académicos, empresários e gestores, técnicos de informática, decisores públicos, etc. – tornou-se comum recorrer a uma frase que se acredita poder servir para sintetizar a importância e a atenção que esta matéria deve merecer por parte dos múltiplos

atores, e em especial pelas empresas: "só existem dois tipos de empresas: as que já foram atacadas, e aquelas que ainda não sabem que já foram atacadas"[1].

É neste quadro em que a transformação digital e, em especial, o ciberespaço acrescentam uma difusão de poder entre múltiplos atores, onde as sociedades e as suas economias dependem cada vez mais da tecnologia e de plataformas de comunicação como a Internet, que as políticas públicas adquirem um papel de destaque na prossecução do bem-estar e na proteção do Estado.

Tendo por pano de fundo os potenciais riscos para as empresas associados à transformação digital, nomeadamente aqueles que resultam de vulnerabilidade das empresas a ataques intencionais e não intencionais, resultando em eventual roubo de informação, disrupção da atividade, dano na reputação, etc., partimos para este trabalho com uma interrogação: "como estão as empresas portuguesas, em especial as PME, a lidar com os riscos de cibersegurança e que papel desempenha o Estado, ao nível das políticas públicas, nessa ação". Dado o limitado número de trabalhos disponíveis focados exclusivamente no setor empresarial português que nos permitisse verificar como as empresas, e, uma vez mais, em particular as PME, estão a percecionar e a avaliar os riscos, assim como a implementar medidas, resultantes ou não de eventuais políticas públicas nesta área, fomos forçados a reformular a nossa pergunta de partida. Limitados no tempo para este trabalho, focamo-nos em quadros teóricos, estudos e inquéritos internacionais existentes na espectativa de contribuir, no fim, com orientações passíveis de serem adotadas por empresas. Para esse fim, procurámos responder à pergunta: "como poderão as empresas portuguesas, em especial as PME, lidar com os riscos de cibersegurança e, face ao quadro de políticas públicas nacional e internacional, que instrumentos têm ao seu dispor para tal?".

No capítulo I procuramos desenvolver um enquadramento teórico abordando as questões da transformação digital e a sua relação com a economia, primeiro num quadro internacional e depois no quadro nacional, as suas implicações e também a relação das PME e a cibersegurança. O capítulo II ficou reservado para a apresentação metodológica e o quadro de análise deste trabalho onde, recorrendo à bibliografia existente, apresentamos a orientação conceptual utilizada neste trabalho. Os resultados e discussão de toda a informação possível de recolher foram abordados no capítulo III, onde procurámos consolidar áreas que consideramos de extrema relevância na relação entre as organizações, em especial as empresas, e a cibersegurança. Finalmente, o capítulo final apresenta as principais conclusões a que fomos conduzidos pelo estudo que fomos desenvolvendo. Neste capítulo de conclusões não sentimos qualquer inibição na apresentação de uma proposta de trabalho futuro em termos de políticas públicas para área da cibersegurança em Portugal, porque acreditamos que é impreterível que cibersegurança deixe de ser "uma chatice".

[1] Autor desconhecido.

CAPÍTULO I: ENQUADRAMENTO TEÓRICO

I.1. Transformação Digital e a Economia Digital

A permanente necessidade de periodização e caracterização histórica que permita uma melhor perceção das fronteiras e etapas do processo evolutivo das sociedades é passível de colocar determinados processos em situação de ambiguidade. É o caso da conceptualização sobre as revoluções industriais. Se encontramos teóricos que sustentam que o atual momento, em termos de desenvolvimento social e económico, é o resultado de uma terceira revolução industrial (Rifkin, 2016; Robert Gordon em Zigler, 2017), outros consideram-no como o fruto duma quarta revolução industrial em curso (Comissão Europeia, 2016; EPRS, 2016; WEF, 2016; OCDE, 2017a; Schwab, 2017a). Não sendo o nosso objetivo enveredar por uma discussão conceptual sobre a sua periodização, torna-se evidente que a origem destas diferenças se encontra na interpretação que os teóricos fazem das alterações tecnológicas, identificando, dessa forma, diferentes momentos de transformação.

Independentemente de se considerar a linha teórica que defende a ocorrência da primeira revolução industrial nos séculos XVIII e XIX, a segunda no século XX e a terceira no século XXI, ou a linha teórica que considera a primeira revolução industrial no século XVIII, a segunda no século XIX, a terceira no século XX e a quarta no século XXI, parecem existir evidências de que qualquer uma das duas linhas teóricas apresenta, na génese das revoluções, um paralelismo: elas resultam de transformações tecnológicas ao nível da energia, dos transportes, das comunicações[2] e da produção. A profundidade dos trabalhos que sustentam a segunda linha teórica motiva-nos a seguir aqui o entendimento de que as sociedades, neste início do século XXI, e em particular as dos países desenvolvidos, se encontram perante os desafios colocados por uma quarta revolução industrial.

É reconhecido que qualquer uma das revoluções industriais[3] teve um tremendo efeito transformador nas sociedades. Pessoas e bens passaram a dispor de maior mobilidade num menor curto espaço de tempo, as novas fontes de energia permitiram a sua utilização de forma mais intensiva, seja para o bem-estar social, seja para a produção de bens, e a maneira de comunicar tornou-se mais rápida e com mais alcance.

Importa desde já, nesta fase do nosso trabalho, clarificar que não fazemos aqui a apologia das TIC, e em especial da Internet como uma plataforma fundamental do seu desenvolvimento, como a transformação tecnológica que até hoje mais terá contribuído para revolucionar a sociedade no seu

[2] Optámos pela utilização do conceito de comunicações e não de telecomunicações dada a sua abrangência, pois considera-se relevante o papel que a escrita impressa desempenhou na primeira revolução industrial.

[3] A terminologia "revolução industrial" para caracterizar estas mudanças de paradigma não nos oferece, neste contexto, qualquer resistência dado que acompanhamos Schwab na interpretação da palavra "revolução": "A palavra "revolução" denota uma mudança abrupta e radical. Ao longo da história, as revoluções aconteceram quando novas tecnologias e novas formas de entender o mundo desencadearam uma profunda mudança nos sistemas económicos e estruturas sociais" (2017a: 9).

todo[4]. Não obstante os paralelos que traçámos atrás, a aferição das transformações produzidas pelas referidas revoluções industriais e, consequentemente, a avaliação do impacto que as tecnologias subjacentes tiveram, e ainda têm, nas sociedades é, no nosso entender, um exercício extremamente difícil de concretizar e que não tem espaço neste trabalho. No entanto, não ignoramos que as TIC e, em especial, a Internet, pela sua dimensão e quase impossibilidade de lhe impor fronteiras, associadas ao fenómeno da globalização, parecem ter vindo intensificar e acelerar os processos de transformação. Também não nos é despercebido um vasto conjunto de estudos que têm vindo a ser realizados ao longo do tempo, e.g. pela Organização para a Cooperação e Desenvolvimento Económico (OCDE) (2010; 2012; 2015; 2017), que parece apontar esta como a transformação que estará a ocorrer a um ritmo mais acelerado. No entanto, sobre este ritmo, parece-nos relevante a observação de Polanyi:

> o ritmo das transformações não é, em muitos casos, menos importante do que a direção em que essas transformações se orientam – mas, embora a direção do processo muitas vezes não dependa da nossa vontade, é possível que dependa do que fizermos o ritmo das transformações em curso.
>
> A fé no progresso espontâneo torna-nos necessariamente cegos para o papel dos governos na vida económica. Esse papel consiste com frequência na modificação do ritmo da mudança, acelerando-o ou abrandando-o conforme os casos: mas se acreditarmos que o ritmo em causa é inalterável – ou, pior ainda, se considerarmos um sacrilégio qualquer tentativa de interferência nele – então, sem dúvida, não nos restará qualquer margem de manobra (Polanyi, 2012: 166-167).

Sendo a inovação tecnológica apresentada como uma das componentes fundamentais para a competitividade (Lopes, 2001) – e aqui, ainda que simplisticamente, podemos considerar tecnologia como "formas atualmente conhecidas de converter recursos em resultados desejados pela economia" (Griliches, 1987 citado em OCDE, 2001: 11) –, o desenvolvimento das TIC é altamente impulsionado por incentivos políticos e financeiros (Toffler, 1991; MSI, 1997; Salavisa Lança, *et al.*, 2004; 2005; Castells, 2011; Mazzucatto, 2014; Cardoso, *et al.*, 2015; Ferreira, 2015; Nunes, 2015; Rifkin, 2016;

[4] Importa referir que nesta matéria existem posições antagónicas sobre o impacto da tecnologia. Em oposição aos que defendem o poder revolucionário das TIC e da Internet, encontram-se aqueles que, não negando um impacto considerável, colocam algumas reservas sobre o seu poder revolucionário. Por exemplo, Ha-Joon Chang (2010) serve-se do exemplo de eletrodomésticos, como a máquina de lavar ou o aspirador, para justificar grandes transformações sociais decorrentes da alteração na força de trabalho: com algumas das tarefas domésticas, habitualmente desempenhadas por empregados(as) domésticos(as), a passarem a poder ser desempenhadas de forma autónoma ou sem a necessidade de contratar pessoas propositadamente para as executar, existiu, no seu entender, uma alteração e libertação de tempo de trabalho provocando transformações laborais e, consequentemente, sociais (Chang, 2010: 31-40). No entanto, deve salientar-se que o autor, àquela data, reconhece não existirem ainda dados suficientes que permitissem afirmar a Internet como a tecnologia com mais impacto no conjunto das tecnologias que originaram os processos de revolução industrial. Outro exemplo é Robert Gordon, um economista norte-americano, que "está entre aqueles que defendem que a revolução digital, por muito impressionante que seja, tem um potencial transformador relativamente limitado, quando comparado com as grandes inovações da segunda metade do século XIX" (Franklin, 2017: 12). Ainda sobre a visão de Robert Gordon ver Zigler, 2017.

Baller, *et al*, 2016; Isaías, *et al.*, 2017). Estes incentivos potenciaram avanços ao nível da investigação e desenvolvimento, permitindo que as TIC e a Internet se assumissem como a raiz de um novo paradigma tecnológico e económico assente no conhecimento. E é a aplicação deste conhecimento que, na ideia de Toffler, adquire um "poder da mais alta qualidade" entendido como não sendo "simplesmente a capacidade de influenciar" mas também implicando "eficiência – utilização do menor número de recursos de poder para alcançar um objetivo", "servindo como multiplicador de riqueza e força", isto é, "utilizado para aumentar a força ou a riqueza disponível ou, alternativamente, para reduzir a quantidade necessária para alcançar um determinado propósito" (1991: 29). "A evolução económica mais importante do nosso tempo tem sido o advento de um novo sistema criador de riqueza, baseado não já nos músculos, mas, sim, na mente" (Toffler, 1991: 21). Na mesma linha, Drucker preconiza que "o desafio *económico* da sociedade pós-capitalista[5] será a produtividade do trabalho e do trabalhador com base no conhecimento" (2015: 22)[6].

Com esta alteração do paradigma social e económico assente na digitalização[7], onde equipamentos e serviços deixam a sua componente de funcionamento maioritariamente analógica e passam a ter características digitais, assistimos ao que se apelida de transformação digital. A transformação digital, entendida como a aplicação das tecnologias digitais em todas as áreas da sociedade, é alimentada com o advento da ligação dos objetos à Internet, a chamada Internet das Coisas, a criação e acumulação, por equipamentos e pessoas, de dados de forma quase ininterrupta e a necessidade de armazenamento e processamento em elevada escala que conduziu à tecnologia de computação em nuvem. Assiste-se hoje em dia à ação disruptiva das tecnologias em áreas que há uns anos se julgavam pertencentes ao domínio da ficção científica, em filmes ou em livros. Hoje são já conhecidos saltos tecnológicos reais e significativos, por exemplo, ao nível de veículos autónomos e interligados, ou de sistemas de gestão de territórios e cidades interligados em redes complexas e automatizadas, conhecidos por cidades inteligentes. Esta transformação, para além do impacto que tem na ação e participação política e social, seja ao nível do comportamento e relação entre pessoas e/ou entre pessoas e o trabalho, tem também um grande impacto ao nível económico. Na forma como as empresas produzem e ainda na forma como estas se relacionam com a economia.

---

[5] Não consideramos, para este trabalho, relevante o aprofundamento ou a explanação sobre a conceptualização de "sociedade pós-capitalista" utilizada por Peter Drucker. No entanto, julgamos pertinente situar cronologicamente o momento em que ocorre, no seu entender, esta visão evolutiva da sociedade assente no conhecimento: "A mudança para a sociedade pós-capitalista iniciou-se logo a seguir à Segunda Guerra Mundial" (Drucker, 2015: 20).

[6] Itálico no original.

[7] É frequente encontrar na bibliografia uma utilização das expressões, no inglês, "digitization" e "digitalization" cuja tradução para o português, para ambas as situações, resulta em digitalização. No entanto, conceptualmente são diferentes. O primeiro conceito refere-se à transformação de sinais analógicos (som, imagem, documentos, etc.) em expressões binárias (uns e zeros) (OCDE, 2017: 24) de forma a ser interpretado por computadores, enquanto o segundo se refere à alteração de processos e bens para, e em plataformas e sistemas digitais ou computorizados. Aqui referimo-nos ao segundo conceito.

A transformação digital, e o seu impacto na economia, conduziu ao "reconhecimento do papel do conhecimento e da tecnologia no crescimento económico" (OCDE, 1996: 9). Estas novas economias baseadas no conhecimento (OCDE, 1996) ganharam a designação técnica de "economia digital" dada a "passagem do modelo de «economia baseada no átomo» no sentido de material massa ou transporte para o modelo *bits* baseado na criação, manipulação, comunicação e armazenamento de dígitos binários eletrónicos" (Isaías, *et al.*, 2017: 53)[8]. No entanto, atualmente, a expressão "economia digital" não se cinge à mera especificidade técnica e assume uma visão conceptual bastante abrangente: "uma economia do conhecimento baseada no digital", isto é, uma economia caracterizada "pela existência de redes e infraestruturas de comunicação digital que fornecem uma plataforma global onde as pessoas e as organizações definem estratégias, interagem, comunicam, colaboram e procuram informações para atuações coletivas ou conjuntas" (Isaías, *et al.*, 2017: 53).

A dependência da economia de plataformas digitais, com elevada influência nos modelos de negócio, processos de produção e serviços, é reconhecida, com alguma frequência, em estudos que pretendem avaliar o seu impacto. A título de exemplo, em Baller, *et al*. é salientado que "o desenvolvimento da Internet comercial tem ocorrido simultaneamente com a expansão massiva da economia global, evidenciando um crescimento superior de 6,6 vezes em termos nominais – de 11,1 biliões de dólares para 73,3 biliões de dólares[9] desde 1980" (2016: 39). Ou ainda, que na União Europeia as exportações com origem na economia digital, em 2012, representaram um ganho na ordem dos 465 mil milhões de dólares e as importações, pela mesma via, um gasto de cerca de 297 mil milhões de dólares (Baller, *et al.*, 2016: 39). O lançamento da Estratégia para o Mercado Único Digital na Europa (Comissão Europeia, 2015), entre os seus vários pressupostos, assumia que esta se tornaria a base para "as empresas poderem explorar plenamente as novas tecnologias e para as pequenas empresas em particular poderem atravessar a União Europeia (UE) «apenas num clique»", representando um possível "contributo de 415 mil milhões de euros adicionais por ano para a nossa economia e criar centenas de milhares de novos empregos" (Comissão Europeia, 2016a: 4). Para além desta tentativa de avaliar a evolução do impacto da transformação digital na economia, há ainda tentativas de previsão desse impacto com base em tendências tecnológicas como a análise massiva de dados e a computação em nuvem para dados em grande escala. Neste campo, o World Economic Forum (WEF) prevê que a utilização destas tecnologias possa representar uma fonte de criação de valor "entre 9,6 biliões de dólares e 21,6 biliões para a economia global" (WEF, 2014: 3).

Não obstante os vários indicadores disponíveis para avaliar algumas das características específicas que constituem a economia digital (OCDE, 2002; 2010; 2012; 2015; 2017; Ferreira, 2015;

[8] Itálico no original.

[9] Dada a opção, neste trabalho, pela apresentação das citações extraídas da bibliografia traduzidas para a língua portuguesa, reconhecemos a importância, nesta fase do texto, de esclarecer que as referências a numerais seguirão a regra definida em Portugal resultante da convenção estabelecida na 9.ª Conferência Geral de Pesos e Medidas que decorreu entre 12 e 21 de outubro de 1948. Assim, em rigor com essa regra, serão traduzidas todas as expressões numéricas, como neste caso específico, do original "from US$11.1 trillion to US$73.3 trillion" para "de 11,1 biliões de dólares para 73,3 biliões de dólares". Sobre esta regra, ver https://www.flip.pt/Duvidas-Linguisticas/Duvida-Linguistica/DID/4389 consultado em 30 de novembro de 2017.

UNCTAD, 2017), é reconhecidamente difícil avaliar o peso que esta, como um todo, tem no PIB nacional e, consequentemente, mundial (Brynjolfsson e Kahin, 2000; OCDE, 2014; Quiggin, 2014; Ahmad e Schreyer, 2016). Não existindo espaço neste trabalho para o aprofundamento desta discussão, é largamente aceite, mesmo perante essa complexidade de aferição, e à qual acrescem ainda as abordagens sobre a economia digital de bens livres (Nakamura, *et al.*, 2017) ou de custo marginal zero (Rifkin, 2016), que o peso da economia digital na economia dos países e das regiões é relevante em termos económicos e com um impacto significativamente elevado. A atestar essa tendência, estão as apostas dos governos e das organizações internacionais na definição e implementação de estratégias de âmbito nacional e internacional (e.g. OCDE, 2010; 2012; 2015; 2017; Comissão Europeia, 2015; 2016) com o objetivo de relacionar o conhecimento e a tecnologia com a economia, confirmando, assim, a crescente dependência das empresas em relação às TIC, e em especial em relação à Internet.

Mas se são reconhecidos os benefícios da economia digital para o crescimento (Jorgenson e Vu, 2016) e desenvolvimento económico dos países e regiões, os riscos e as ameaças a que está sujeita são igualmente objeto de tentativa de análise e exposição na bibliografia atual proveniente não só de organizações públicas e das comunidades técnica e académica mas também do setor privado.

Tendo surgido, no início do século XXI, preocupações com as perdas para a economia resultantes de ações nos ambientes digitais, quase em simultâneo com a massificação da utilização da Internet[10] como plataforma comercial, e também social, é no final da primeira década que começa a emergir uma maior preocupação com o impacto negativo na economia global decorrente de más práticas, intencionais e não intencionais, na Internet. Daí resulta um conjunto de iniciativas nacionais e internacionais com vista à eliminação e mitigação dos riscos que acompanham a transformação digital. Em 2009, a Comissão Europeia salientava um estudo do WEF, de 2008, em que apontava para custos económicos globais na ordem dos 250 mil milhões de dólares em resultado, apenas, de roturas ao nível de infraestruturas críticas de informação[11], cuja probabilidade de concretização, num prazo de 10 anos,

[10] Um exemplo dessas primeiras preocupações pode ser encontrado na resolução 57/239 da Assembleia Geral das Nações Unidas, adotada em janeiro de 2003, no seguimento da 78.ª Reunião Plenária de 20 de dezembro de 2002, onde é reconhecido que "em resultado do aumento da interconetividade, sistemas de informação e redes estão agora expostas a um número crescente e a maior variedade de ameaças e vulnerabilidade que levantam novas questões de segurança para todos" (ONU, 2003: 2).

[11] Neste trabalho acompanharemos a definição de infraestruturas de informação crítica estabelecida no âmbito da OCDE: "devem ser entendidas como referentes a sistemas e redes de informação interligados, cuja disrupção ou destruição teria um grave impacto na saúde, segurança ou no bem-estar económico dos cidadãos, ou no funcionamento efetivo do governo ou da economia" (OCDE, 2008: 4). Para mais informações sobre "infraestruturas críticas de informação" ver Diretiva 2008/114/CE do Conselho, de 8 de Dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008L0114. Sobre "infraestruturas críticas" ver Programa Europeu de Proteção das Infraestruturas Críticas disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al33260

se encontraria num intervalo "de 10 a 20%" (Comissão Europeia, 2009: 2). Em 2012, uma comunicação da Comissão Europeia sobre criminalidade na era digital, salientava um relatório da empresa norte americana Symantec dando conta, em 2011, "que as vítimas do cibercrime perdem anualmente cerca de 388 mil milhões de dólares em todo o mundo" (Comissão Europeia, 2012: 2). Ainda à data de 2012, a European Union Agency for Network and Information Security (ENISA) salientava um conjunto de situações potenciadoras de impacto económico e social com efeitos negativos em consequência de incidentes de segurança:

- em 2010, o sequestro de 15% do tráfego mundial da Internet por parte de um operador de telecomunicações proveniente da China;
- em 2011, a falha de segurança de uma autoridade de certificação holandesa;
- em 2011, uma falha de segurança num centro de dados de um fornecedor de uma marca de telefones inteligentes;
- em 2011, uma tempestade na Noruega que provocou uma ausência de comunicações, incluindo Internet, durante duas semanas;
- em 2012, uma quebra de segurança que terá estado na origem da publicação de 6,5 milhões de palavras-chave de uma rede social com enfoque empresarial (ENISA, 2012)[12].

Dado os seus contornos, são também conhecidas situações mediaticamente relevadas como o caso da Estónia, em 2007, e da Geórgia, em 2008, (Santos, 2011), em que alegadamente é ultrapassada a esfera do ataque ou a perpetração dum ato criminoso por parte de organizações ou indivíduos, e se passa para a esfera dos Estados. Nesta linha, há ainda o caso do alegado ataque, em 2014, da Coreia do Norte à empresa Sony Pictures Entertainment (Solomon em Canadian Institute of Actuaries, 2017: 4) ou o reconhecimento mútuo dos Estados Unidos da América (EUA) e da China, em 2015, do impacto que as atividades criminosas no ciberespaço[13] podem ter nas economias. Este último caso tem como resultado a cooperação, ao mais alto nível, de ambos os países em diversos aspetos relacionados com a cibersegurança, mas, acima de tudo, no acordo de "que nenhum dos governos dos países conduzirá ou apoiará de forma consciente o roubo de propriedade intelectual por vias cibernéticas, incluindo segredos comerciais ou outras informações comerciais confidenciais, com a intenção de oferecer vantagens competitivas para empresas ou setores comerciais" (The White House, 2015). O caso da empresa proprietária do sítio da Internet "Ashley Madison" ficou também conhecido pela quebra de segurança que terá exposto informações de cerca de 33 milhões de contas de utilizadores (Hackett, 2015; Hern e Gibbs, 2015). No início de 2017, foram detetados mais de 400 mil computadores infetados, em mais de 150 países, com um software de sequestro designado Wannacry (Comissão Europeia, 2017: 2). No último trimestre de 2017, foi relatada a situação de um ataque

[12] Outros exemplos de incidentes de grande escala podem ser encontrados em OCDE, 2015a: 25.

[13] Conceito que abordaremos mais adiante.

informático concretizado à empresa UBER, durante o ano 2016, e em que esta terá optado por omiti-lo aos seus clientes, dada a transferência de informações sobre cerca de 57 milhões de clientes e fornecedores de serviços para as mãos de criminosos (Newcomer, 2017). Ainda em 2017, foi também notícia a exposição acidental, por via de uma empresa subcontratada pelo Partido Republicano dos EUA, de dados de cerca de 200 milhões de cidadãos (BBC, 2017). Mais recentemente, entre outros, ficou a conhecer-se os casos da violação de dados de cerca de 143 milhões de clientes da empresa norte-americana Equifax, maioritariamente provenientes dos EUA, mas também do Canadá e do Reino Unido (BBC, 2017a), e de um ataque com o objetivo de sequestrar os sistemas do aeroporto de Bristol (BBC, 2018), em 2018, tendo provocado a disrupção de alguns serviços.

Sendo estes casos um curto exemplo daqueles que têm um impacto mais mediático, as situações de ataques a organizações e pessoas multiplicam-se na ordem dos milhares por dia (Rettman, 2017).

Não obstante os diversos exercícios de contabilização dos custos e perdas para a economia resultante de incidentes, especialmente relacionados com a utilização de plataformas e redes digitais, é frequente encontrar-se um vazio de informação. Para alguns dos incidentes que ficam a ser conhecidos, existe um défice de informação quanto ao impacto que estes provocam[14], tanto na economia como nas próprias empresas, mesmo que exista a perceção de que esse impacto é verdadeiramente nefasto. E esta falta de informação resulta, acima de tudo, de uma dificuldade relacionada com assimetrias de informação, isto é, uma boa parte da informação relevante para avaliar o verdadeiro custo resultante de atividades criminosas é mantida em segredo por parte das empresas alvo desses ataques e até mesmo pelas entidades responsáveis pela investigação (Moore, 2010). Em qualquer um dos casos, por razões diferentes:

> existe, em geral, um incentivo para não reportar incidentes. Os bancos não querem revelar perdas por via de fraude pelo medo de assustar os clientes da banca online; as empresas não querem cooperar com a polícia em incidentes de ciberespionagem porque a sua reputação (e o preço das ações) pode ser abalada; os operadores de infraestruturas críticas não querem revelar informações sobre interrupções causadas por ataques maliciosos pelo medo de chamar a atenção para vulnerabilidades sistémicas. A reticência para compartilhar informações é apenas contrariada pelo excesso de entusiasmo de muitos na indústria de segurança de TI para exagerar ameaças. (Moore, 2010: 106)

Verifica-se, portanto, que na sequência da exploração de vulnerabilidades, as organizações vêem-se confrontadas com potenciais consequências sociais e económicas ao nível financeiro e de reputação. Mas Moore chama a atenção para o facto de que a "existência de uma assimetria de informação não significa necessariamente que a sociedade não esteja a investir o suficiente em segurança" (2010: 106), assumindo que esta assimetria de informação contribua, talvez, para o desconhecimento da proporção e do destino correto destes investimentos que, como vimos acima, atingem já uma dimensão supranacional.

[14] Cf. Canadian Institute of Actuaries, 2017.

Independentemente das motivações e dos objetivos subjacentes à exploração das vulnerabilidades e concretização de ataques, como veremos mais adiante, especialmente direcionados às empresas, os métodos utilizados podem variar no tipo e na escala (Kim, *et al*., 2010; Glenny, 2011; ENISA, 2012; 2017; OCDE, 2012a; 2015a; Rotenberg, *et al.*, 2015; Schneier, 2015; Nunes, 2016; Cisco, 2017; Comissão Europeia, 2017a; Thomas, *et al*., 2017). Neste campo, em consequência dos impactos económicos negativos a que já aludimos anteriormente, e à constatação da impreparação que pessoas e empresas manifestam perante a exploração de vulnerabilidades (MARSH, 2016; Cisco, 2017; EY, 2016), tem-se assistido ao proliferar de um conjunto de iniciativas que visam dotar os Estados e as empresas de mecanismos de preparação, proteção e resposta a incidentes no ciberespaço. Para além de iniciativas postas em prática por governos nacionais, salientam-se, a nível da UE, quatro iniciativas emblemáticas recentes[15] visando alcançar níveis elevados de proteção da economia, nomeadamente em organizações do setor público e privado[16]:

- A Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido (Comissão Europeia 2013; Matos, 2015);
- A Estratégia para o Mercado Único Digital na Europa (Comissão Europeia, 2015);
- A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JOUE, 2016a);
- A Comunicação "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE" (Comissão Europeia, 2017).

Estas iniciativas pretendem não só alavancar o processo de transformação digital na UE, e em especial o crescimento da economia digital, mas também fazê-lo acompanhar de medidas que promovam ambientes de segurança e confiança para empresas, cidadãos e governos. O foco destas centra-se em matérias de desenvolvimento de uma indústria europeia de cibersegurança com o objetivo de tornar a Europa numa região capaz de competir com outros atores de maior domínio, como os EUA; de dotar as entidades públicas e autoridades de meios e instrumentos para mitigar e responder a incidentes nacionais e transnacionais na UE; de capacitar profissionais para responder aos desafios impostos pelo avanço tecnológico; e ainda de adotar medidas legais e técnicas que permitam às empresas, no âmbito das suas atividades comerciais, ultrapassar determinadas barreiras impostas pela geografia e quadros regulamentares diferentes dentro da própria UE.

[15] Neste trabalho dispensamo-nos de apresentar um registo histórico extenso do surgimento e evolução de iniciativas nacionais e, principalmente, europeias em matéria de cibersegurança (cf. Comissão Europeia, 2013; JOUE, 2016a).

[16] Nesta matéria de cibersegurança, estamos propositadamente a excluir as iniciativas postas em prática que visam exclusivamente a proteção dos cidadãos, pese embora as iniciativas destacadas terem também em consideração aspetos dessa natureza.

Algo que também esteve sempre presente como incentivo em matéria de cibersegurança, e que sai ainda mais reforçado com a Comunicação "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE" (Comissão Europeia, 2017)[17], é a questão da investigação e desenvolvimento (I&D). As prioridades apresentadas pela Comissão Europeia nesta Comunicação pressupõem um maior empenho dos Estados-Membros no desenvolvimento de centros de excelência em competências e investigação científica nesta matéria, assim como mais investimento público e privado. No entanto, não deve ignorar-se que, ao longo dos anos, a UE tem dotado os seus Programas-Quadro de Inovação e Desenvolvimento Tecnológico de algumas linhas de financiamento com vista a apoiar projetos que desenvolvam soluções e ações relacionadas com a cibersegurança. Não vamos, porque não é o âmbito deste trabalho, questionar a eficácia e assertividade dessas linhas de financiamento, nem mesmo a sustentabilidade dos projetos financiados após o término do período de financiamento. Limitamo-nos a sublinhar a importância da I&D e, principalmente, a transversalidade de que se reveste, para a cibersegurança e para o alcance de elevados níveis de proteção e confiança na utilização da Internet e da tecnologia.

Como vimos até aqui, o processo de transformação digital tem sido acompanhado por incentivos ao desenvolvimento de tecnologias e soluções para responder aos desafios, quase diários, impostos pela sociedade ao nível social, económico e político. E esses incentivos, nomeadamente ao nível da UE, passam em grande medida pela transformação do setor industrial dado o entendimento que

> todos os setores da indústria podem tirar partido dos pontos fortes da Europa no domínio das tecnologias digitais para o desenvolvimento dos mercados profissionais, tais como eletrónica para o setor automóvel, cuidados de saúde e mercados da energia, equipamentos de telecomunicações, software de gestão e fabrico avançado. Há também domínios em que são necessários progressos, nomeadamente no que respeita ao nível de investimento das pequenas empresas em tecnologias da informação e das comunicações (TIC), à oferta de produtos de consumo digitais e aos serviços Web. Na Europa, os setores de alta tecnologia estão bastante avançados na aplicação de inovações digitais, mas grande parte das PME, das empresas de média capitalização e dos setores não tecnológicos ainda estão atrasados. Existem também grandes disparidades entre regiões no que respeita à digitalização (Comissão Europeia, 2016: 2).

É neste quadro que assenta a Comunicação "Digitalização da Indústria Europeia – Usufruir de todos os benefícios do Mercado Único Digital" (Comissão Europeia, 2016) apresentando um "conjunto de medidas políticas coerentes no âmbito de um pacote de modernização das tecnologias e dos

[17] Em setembro de 2017, e na linha de reforço destas matérias, a Comissão Europeia iniciou um novo processo legislativo ordinário com a proposta (COM(2017) 477 final) de "Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)" (Comissão Europeia, 2017b). Não obstante o reforço institucional e técnico ao nível europeu que esta proposta pretende incrementar, uma vez que à data em que desenvolvemos o nosso estudo esta ainda se encontra na fase inicial desse processo, escusamo-nos de a analisar profundamente. Isso não implica, no entanto, que não possamos recorrer ao seu conteúdo sempre que entendermos ser conveniente para este trabalho.

serviços públicos" (Comissão Europeia, 2016: 3) apostando no desenvolvimento da indústria europeia por via de um plano de criação de uma infraestrutura de computação em nuvem à escala europeia; em prioridades em termos de normalização das TIC; no desenvolvimento de ações para a transformação digital nas Administrações Públicas para dar resposta às necessidades dos cidadãos e das empresas; e, por fim, no reconhecimento dos desafios e oportunidades inerentes à Internet das Coisas.

Por forma a criar condições para a competitividade das empresas e das regiões, esta aposta na transformação digital das empresas – através da produção, processos e modelos de negócio – com o objetivo de criar um impacto positivo ao nível da economia com o desenvolvimento das tecnologias digitais e criação de emprego, tem servido de motor para a replicação de iniciativas nacionais focadas na industrialização. Neste sentido, em março de 2017, por altura da comemoração dos 60 anos da UE, foi lançada uma Plataforma Europeia de iniciativas nacionais, com vista à coordenação destas entre Estados-Membros da UE, e à qual se verificou a adesão de 13 países que já haviam implementado iniciativas de transformação digital da indústria. Poucos meses depois, em dezembro de 2017, estavam identificadas estratégias nacionais de 15 países: Alemanha, Áustria, Bélgica, Dinamarca, Espanha, França, Holanda, Hungria, Itália, Lituânia, Luxemburgo, Polónia, Portugal, República Checa e Suécia[18].

Analisaremos em seguida o enquadramento português nestas matérias.

I.2. Economia Digital em Portugal

Importa, desde já, ter presente que

> organizações internacionais, como a OCDE ou as agências especializadas da ONU (incluindo o FMI), europeias, como o Conselho da Europa, ou da União Europeia […], com destaque para a Comissão Europeia, influenciam cada vez mais as políticas nacionais, seja de forma indireta através de processos de imitação e emulação por parte dos atores nacionais (adoção de conceitos comuns, replicação de "boas práticas", etc.), seja de modo direto e coercivo, através de condicionalidades formais (princípios, regras) ou instrumentais (no caso da UE: incentivos, iniciativas e programas comunitários, etc.) (Ferrão, 2015: 330).

Ainda, que no quadro da UE, a definição da agenda política, e consequente processo de elaboração e implementação de políticas públicas, é determinada por um conjunto de fatores que vão desde obrigações impostas por tratados a emergências ou crises passando, por exemplo, por pressões de harmonização entre Estados-Membros ou legislativas (Matos, 2015: 38-41).

Apesar de ter, desde muito cedo, estabelecido a visão de que a Sociedade da Informação se trata de "uma sociedade de mercado" onde "as empresas que lhe irão dar corpo, grande parte delas ainda não criadas, obedecem a novos paradigmas" que, "dotadas necessariamente de uma grande capacidade criativa, devem poder dispor de um espaço regulamentar que lhes permita potenciar essa característica" (MSI, 1997: 39), Portugal, em matérias de transformação digital, não difere de outros

[18] Cf. https://ec.europa.eu/digital-single-market/en/cordination-european-national-regional-initiatives, consultado em 10 de dezembro de 2017.

países no que respeita aos estímulos para o desenvolvimento da economia digital. Para esse efeito, e dada a região, geográfica e política, onde está inserido, muitas das medidas de incentivo à transformação digital das empresas, e também da sociedade, surgem como uma resposta a orientações provenientes da UE ou parecem estar alinhadas com medidas que, mesmo tendo a sua génese noutros países, são consideradas como referências de boas práticas. Estas orientações com origem no quadro europeu resultam, em grande medida, da tentativa da UE em corrigir assimetrias em termos de competitividade e de desenvolvimento económico em relação a outras regiões mundiais, em especial os EUA e alguns países da região asiática. Estas assimetrias, que atualmente ainda são possíveis encontrar, dado o domínio presencial e influência global de algumas empresas norte-americanas e asiáticas no processo de transformação digital, e que são frequentemente reconhecidas em documentos da União Europeia, historicamente parecem resultar da "fraca capacidade de investir nas várias modalidades do novo investimento, seja ele em tecnologias de informação e comunicação, seja ele em conhecimento" (Salavisa Lança e Valente, 2005: 63), em especial num momento crítico como o do início da quarta revolução industrial, isto é, na passagem do século XX para o século XXI[19].

No entanto, o quadro nacional em termos de transformação digital apresenta algumas peculiaridades que importa registar. Neste exercício não pode, de forma alguma, ser ignorado o atraso social e económico a que Portugal esteve sujeito durante várias décadas, durante a ditadura do Estado Novo[20], entre 1933 e 1974, e logo imediatamente a seguir à revolução de abril de 1974, nomeadamente pelos seus elevados índices de iliteracia e níveis de desenvolvimento tecnológico ao nível dos países mais pobres do mundo ocidental. Uma evidência dessa situação de atraso relativamente a outros é, por exemplo, como salientam Godinho e Mamede, o facto de que em Portugal, "em 1980, a percentagem da força de trabalho na agricultura continuava a ser de 24%" (2016: 333)[21].Uma situação que colocou Portugal numa posição de partida bastante inferior a alguns dos seus atuais parceiros na UE.

Com um caminho percorrido em pouco mais de quatro décadas de democracia e pouco mais de três décadas de participação na UE, Portugal, confrontado com o fenómeno da globalização e com o processo de transformação digital, segundo os dados do INE relativos a 2017, apresenta-se com mais

[19] Sobre a relevância do investimento em I&D, público e privado, para o desenvolvimento tecnológico das economias bem como os desequilíbrios que se verificam nesta matéria colocando países e/ou regiões em posição de vantagem em relação a outros/outras em termos de processos de transformação digital ver Salavisa Lança e Valente., 2005; Eurostat, 2013; Mazzucato, 2014; OCDE, 2017.

[20] Não obstante Portugal ter vivido sob um regime ditatorial entre 1926 e 1974, a academia estabelece neste período, pelas suas características de governo, a existência de dois regimes distintos: a "Ditadura", entre 1926 e 1933 e o "Estado Novo" de 1933 a 1974 (Marques, 1998: 377-387).

[21] No trabalho de Godinho e Mamede (2016) um dos indicadores utilizados na constatação do atraso de Portugal em relação à Itália, em termos de política industrial, é a percentagem da força de trabalho ainda afeta ao setor agrícola em ambos os países em 1980: enquanto em Portugal esse valor se fixava nos 24%, praticamente um quarto da totalidade da força de trabalho portuguesa, em Itália o valor era 13%.

de um quarto da população que não utiliza a Internet regularmente[22] ficando, em termos comparativos na UE a 28 países, apenas à frente da Roménia, Bulgária, Grécia e Itália, segundo o Digital Economy & Society Index (DESI) da UE[23]. Ainda segundo o DESI, em termos de competências digitais básicas, Portugal também se encontra abaixo da média europeia, 47,6% e 56,2% respetivamente, bem como ao nível de especialistas em TIC empregados, 2,3% contra 3,5%. No entanto, em termos de digitalização das empresas, um indicador calculado a partir de várias subdimensões relacionadas com as empresas[24], o resultado apurado pelo DESI coloca Portugal, com 14,6%, acima da média europeia de 11,9%, ficando atrás apenas de países como a Alemanha, Bélgica, Dinamarca e Holanda. Em termos de comércio eletrónico[25], Portugal, com 18,2%, surge ligeiramente acima da média europeia, de 17,4%, posicionando-se à frente de países considerados tecnologicamente mais avançados como a Áustria, França, Holanda e até a Estónia, muitas vezes dada como exemplo da transformação digital ao nível social e do setor público (A.A.K., 2013; Lember, *et al.*, 2018).

Para fazer face aos desafios da transformação digital e tentar superar problemas relacionados com a competitividade das empresas, estando ainda muito presente o recente processo de intervenção financeira externa a que Portugal esteve sujeito entre maio de 2011 e maio de 2014, com consequências na tomada de decisão nacional (Godinho e Mamede, 2016), nos últimos anos tem-se assistido à implementação de políticas públicas maioritariamente em resposta a estímulos recebidos pelas diretrizes europeias.

Em Portugal, atualmente[26], as medidas de estímulo ao desenvolvimento da economia digital estão, principalmente, refletidas em iniciativas como:

---

[22] Os dados consultados em 10 de dezembro de 2017 relativos ao "Inquérito à utilização de TIC pelas famílias" do INE, aponta para o total de 73,8% a "Proporção de indivíduos com idade entre 16 e 74 anos que utilizaram Internet nos primeiros 3 meses do ano (%)".

[23] O DESI – Digital Economy & Society Index, anteriormente designado por Digital Agenda Scoreboard da UE, agrega um conjunto de indicadores relacionados com as prioridades digitais da UE. Importa salientar que na nossa análise da proporção de indivíduos que utiliza a Internet, detetámos uma discrepância entre o valor indicado pelo INE (73,8%) e o valor indicado pelo DESI (68,0%) relativamente ao ano de 2017. Admitimos, no entanto, esta diferença dado o facto do valor indicado pelo INE conter uma chamada de atenção para uma atualização a 21 de novembro de 2017. O DESI pode ser consultado em https://digital-agenda-data.eu/

[24] O resultado deste indicador resulta da medição de cinco subdimensões relacionadas com as empresas, todas elas com a mesma ponderação (20% cada) no cálculo final: "DESI Business Digitisation sub-dimension calculated as the weighted average of the normalised indicators: 4a1 Electronic Information Sharing (20%), 4a2 RFID [Radio-frequency identification] (20%), 4a3 Social Media (20%), 4a4 eInvoices (20%), 4a5 Cloud (20%)" *in* https://digital-agenda-data.eu/datasets/desi/indicators.

[25] À semelhança de indicadores anteriores, também este resulta de uma agregação de outras subdimensões: "DESI eCommerce sub-dimension calculated as the weighted average of the normalised indicators: 4b1 SMEs Selling Online (33%), 4b2 eCommerce Turnover (33%), 4b3 Selling Online Cross-border (33%)" *in* https://digital-agenda-data.eu/datasets/desi/indicators.

[26] Para uma perspetiva histórica da evolução destes estímulos ver Coelho, 2012 e Ferreira, 2015.

- Portugal 2020[27], que estabelece o enquadramento do financiamento de ações com verbas provenientes dos fundos estruturais e de investimento da União Europeia;
- Agenda Portugal Digital[28], adotada em 2012 e revista em 2015 que sucede à Agenda Digital 2015[29], e que agrega um conjunto de iniciativas setoriais para o desenvolvimento da economia e sociedade em torno do digital como resposta a uma condicionante imposta pela UE na atribuição de fundos estruturais;
- Programa Indústria 4.0[30], que tem como principal objetivo "acelerar a adoção da indústria 4.0 pelo tecido empresarial";
- CITec - Programa Capacitar a Indústria Portuguesa[31], que define um conjunto de medidas visando a transferência de conhecimento das instituições de ensino superior para as empresas;
- Portugal INCoDe.2030[32], que prevê que seja desenvolvido um conjunto de ações em resposta aos desafios de competências e qualificações impostos pela transformação digital.

Em Portugal, segundo o INE, em 2016, num universo de 1 214 206 de empresas, se se excluírem as empresas financeiras, verifica-se que o tecido empresarial era composto por 1 196 102 (INE, 2018: 22). Deste número, apenas 1 038 são consideradas grandes empresas pelo que as restantes 1 195 064 são consideradas PME[33], representando, assim, cerca de 99,9% do universo das empresas em Portugal. No entanto, importa ressalvar que apesar desta categorização de PME, é possível verificar que esta maioria é esmagadoramente composta por empresas que pertencem à subcategoria de micro

[27] Cf. https://www.portugal2020.pt, consultado em 2 de dezembro de 2017.

[28] Adotada pela Resolução do Conselho de Ministros n.º 22/2015, de 16 de abril, com o objetivo "estratégico de promover a inovação, o empreendedorismo e a internacionalização da economia nacional, com vista a tornar Portugal um país com empresas de elevado potencial de crescimento e de internacionalização" reafirmando "a relevância da utilização das Tecnologias de Informação e Comunicação (TIC) pelas empresas como fator decisivo para o aumento da sua produtividade e competitividade".

[29] Cf. Presidência do Conselho de Ministros, 2010.

[30] Cf. http://www.i40.pt/, consultado em 2 de dezembro de 2017.

[31] Adotado pela Resolução do Conselho de Ministros n.º 84/2016, de 21 de dezembro.

[32] Cf. http://www.incode2030.gov.pt, consultado em 2 de dezembro de 2017. Na sequência de um processo de revisão e reforço em matéria de competências digitais subsequente ao seu lançamento em abril de 2017, a Portugal INCoDe.2030 foi definida como um programa estratégico do governo através da Resolução de Conselho de Ministros n.º 26/2018, de 8 de março, disponível em http://data.dre.pt/eli/resolconsmin/26/2018/03/08/p/dre/pt/html.

[33] "A categoria das micro, pequenas e médias empresas (PME) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros" (fontes: metainformação INE, consultado em 3 de dezembro de 2017; JOUE, 2003).

empresas, pois "a proporção de empresas com menos de 10 pessoas ao serviço (micro empresas) no total das empresas foi [em 2016] na ordem de 96,2% […]" (INE, 2017a: 31).

No "Inquérito à utilização de TIC nas empresas" de 2017[34], que o INE realiza anualmente, observa-se que, no universo das empresas portuguesas, cerca de 90,5% utiliza computadores, 85,7% tem ligação à Internet[35] e 40,9% tem um sítio da Internet[36]. Segundo o INE, no destaque à comunicação social de 21 de novembro de 2017 sobre o Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas 2017, a proporção de empresas que utilizam comunicações digitais como estratégia de ligação ao mercado é de 46%, "variando entre 44% nas empresas com 10 a 49 pessoas ao serviço, 57% nas empresas de média dimensão", isto é, com 50 a 249 pessoas ao serviço, "e 73% nas grandes empresas", ou seja, nas empresas com 250 ou mais colaboradores (INE, 2017). Ainda segundo o INE, existem mais empresas em 2017 a contratar serviços de computação em nuvem revelando um aumento em relação ao ano anterior: "Em 2017, 23% das empresas referem comprar serviços TIC de computação em nuvem através da internet, o que revela um aumento de 5 p.p. face a 2016. Também esta proporção aumenta com a dimensão da empresa, sendo uma prática referida por 20% das pequenas empresas, 35% das médias empresas e 55% das empresas com 250 ou mais pessoas ao serviço" (INE, 2017).

Este quadro do tecido empresarial português que traçámos de forma pouco exaustiva, visto que destacámos apenas alguns dos indicadores que estão relacionados com o objetivo do nosso estudo, tem, como já o referimos antes, vindo a ser potencialmente influenciado por medidas de incentivo à digitalização das empresas por se acreditar que esta representa um fator transformador principal da competitividade. Um estudo recentemente elaborado pela empresa Impacting Digital, que teve por base um inquérito lançado a mais de 500 empresas, reafirma "que a tecnologia se tem tornado um dos principais condutores das mudanças nas empresas portuguesas, assistindo-se a uma transformação naquilo que são os conhecimentos técnicos dos seus profissionais e na disponibilização de ferramentas para atender às necessidades dos seus clientes" (Sousa, 2018)[37].

---

[34] Neste questionário, o INE informa que "em 2017 passou a recolher-se informação de empresas com 0 pessoas ao serviço" (fonte: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_base_dados: Inovação e Conhecimento > Sociedade da Informação > TIC nas empresas).

[35] Considerando apenas as PME, isto é, de "empresas com 10 ou mais pessoas ao serviço", esta utilização da Internet fica-se pelos 70% (INE, 2017).

[36] Se estes 40,9% se referem a todo o universo das empresas em Portugal, uma vez que, como refere o INE na indicação estatística que disponibiliza, "em 2017 passou a recolher-se informação de empresas com 0 pessoas ao serviço", consultando os dados estatísticos disponibilizados pelo INE para "empresas com 10 ou mais pessoas ao serviço", que fixa nos 65% a proporção de empresas com um sítio da Internet, poderemos assumir que a proporção de micro empresas que tem um sítio da Internet é significativamente baixa. Uma variação que se verifica consoante a dimensão das empresas: 61% em empresas com entre 10 e 49 pessoas, 83% em empresas com entre 50 e 249 pessoas e 96% em empresas com 250 pessoas ou mais (INE, 2017).

[37] Os principais resultados deste estudo encontram-se disponíveis em https://impacting.digital/estudo-transformacao-digital/ consultado em 6 de julho de 2018.

Não podemos deixar de realçar, neste quadro nacional, a dificuldade encontrada na identificação da aferição das políticas públicas que têm vindo a ser implementadas ao longo de algumas décadas. Ou seja, partindo da argumentação disponibilizada pelos documentos que suportam as políticas públicas focadas na transformação digital, mas também não só nesta matéria, parece indiciar uma recorrente tomada de decisão baseada em indicadores disponíveis e não em aprofundados processos de avaliação que permitam compreender como e de que forma esses indicadores de execução foram influenciados por políticas anteriores. Não deve ser, por isso, ignorada a pertinente chamada de atenção de Ferrão sobre as "causas de ineficiência das políticas públicas ao longo das várias fases dos seus ciclos de vida", sendo uma delas a "monitorização baseada em análises quantitativas e indicadores de execução, em detrimento da compreensão dos valores e dos processos institucionais e socioculturais que facilitam ou dificultam a aceitação social das políticas e a obtenção dos resultados desejados" (Ferrão, 2015: 38). Não obstante alguns exercícios de avaliação, ainda que incipientes e levados a cabo, muitas vezes, pelo setor privado ou, quando pelo setor público, pela necessidade de responder a exigências internacionais (Mamede e Feio, 2012; Lopes, 2013; Ferrão, 2015), esta situação parece reforçar a ideia de que existe ainda um "longo e complexo caminho a percorrer no sentido da institucionalização de um sistema de avaliação no nosso país" (Lopes, 2013: 10).

Tendo presente esta constatação, das políticas públicas que destacámos atrás talvez as que mais reflitam a intenção dos decisores públicos em influenciar e intensificar o processo de transformação digital na economia, por via das empresas, sejam o Programa Indústria 4.0 e o Portugal 2020. Mas o destaque destas duas políticas públicas implica que se entenda a diferença de fundo entre ambas.

O Programa Indústria 4.0, ainda que muito alinhado com o movimento europeu nesta matéria[38], consiste numa resposta a desafios identificados principalmente a nível nacional, apresentando um conjunto de medidas e ações definidas com o objetivo de "acelerar a adoção das tecnologias e conceitos da Indústria 4.0 no tecido empresarial português; promover empresas tecnológicas portuguesas a nível internacional; [e] tornar Portugal um polo atrativo para o investimento no contexto Indústria 4.0" (IAPMEI, 2017), para o qual podem ser utilizados alguns dos instrumentos de financiamento disponíveis nos sistemas de incentivos. Já o Portugal 2020 representa o resultado do acordo de parceria entre Portugal e a UE definindo a programação e atuação dos Fundos Europeus Estruturais e de Investimento da UE, isto é, trata-se do programa que define a aplicação do financiamento proveniente da UE para um conjunto de áreas com vista ao desenvolvimento económico, social e territorial de Portugal para o período de 2014 a 2020.

Com cinco objetivos estratégicos e estruturado em seis eixos prioritários (COMPETE 2020, 2015a), o "Programa Operacional Competitividade e Internacionalização" designado por COMPETE 2020 – um dos 16 programas operacionais que constituem o Portugal 2020 – é aquele que estabelece,

[38] Cf. Comissão Europeia, 2016.

em grande medida, as regras de financiamento de ações relacionadas com a transformação digital nas empresas[39]. O COMPETE 2020 visa

> contribuir para a criação de uma economia mais competitiva, baseada em atividades intensivas em conhecimento, na aposta de bens e serviços transacionáveis ou internacionalizáveis e no reforço da qualificação e da orientação exportadora das empresas portuguesas, promovendo igualmente a redução de custos associada a uma maior eficiência dos serviços públicos e à melhoria dos transportes (COMPETE 2020, 2015).

Na edição número 29 do "Ponto de Situação Sistemas de Incentivos às Empresas Portugal 2020", com dados reportados a 30 de novembro de 2017, é possível observar que das 29 216 candidaturas no sistema de incentivos para as empresas[40], apenas 952 foram submetidas por grandes empresas e as restantes 28 264 submetidas por PME representando, em termos de projetos aprovados, cerca de 80% dos incentivos (COMPETE 2020, 2017: 8). Com uma clara noção de que nem todas as candidaturas submetidas dizem diretamente respeito a ações relacionadas com a transformação digital das empresas, estes dados parecem indiciar um grau elevado de atenção, principalmente pelas PME, em relação aos instrumentos públicos disponibilizados para fazer face aos desafios da competitividade das empresas.

Sendo que existe uma manifesta vontade "para colocar Portugal na liderança da Economia Digital na União Europeia" (Presidência do Conselho de Ministros, 2015) e, ao mesmo tempo, parece existir alguma recetividade por parte das empresas para se envolverem em processos de transformação digital, se forem levados em consideração os impactos dessa transformação que expusemos na secção anterior deste capítulo, bem como os dados que realçamos em relação ao quadro nacional, há questões que se levantam e que deverão ser alvo de alguma reflexão.

Se as empresas estão a receber estímulos para se envolverem em processos de transformação digital e para adaptarem as suas estratégias ao nível da empresa, isto é, nas suas estruturas, organização e produção, em função desses estímulos por forma a se adaptarem à economia digital, como estarão elas a considerar esta transformação em termos das estratégias ao nível funcional? Ou seja, se os estímulos à transformação digital determinam a escolha "em que produtos, em que indústrias ou em que países a empresa deve investir os seus recursos, com vista a desempenhar a sua missão e atingir os objetivos organizacionais" (Mações, 2017: 39), como estarão as empresas a encarar

[39] Para além do COMPETE 2020, existem ainda linhas de financiamento para as empresas, ainda que com regras e montantes distintos, nos seguintes Programas Operacionais Regionais no Continente: Programa Operacional da Região do Norte – NORTE 2020, Programa Operacional Regional do Centro – CENTRO 2020; Programa Operacional da Região de Lisboa – LISBOA 2020; Programa Operacional Regional do Alentejo – ALENTEJO 2020; e Programa Operacional CRESC Algarve 2020.

[40] Este sistema de incentivos compreende as linhas de financiamento disponibilizadas pelos programas operacionais COMPETE 2020, NORTE 2020, CENTRO 2020; LISBOA 2020; ALENTEJO 2020 e o CRESC Algarve 2020.

aspetos estratégicos de nível funcional[41] como: a gestão de compras, nomeadamente dos equipamentos para responder aos desafios tecnológicos; a gestão de recursos humanos, para responder à crescente necessidade de competências e formação decorrente dos processos de digitalização; a gestão financeira, para fazer a avaliação das vantagens e dos riscos associados à transformação digital; ou até mesmo a gestão de marketing, para responder às questões de confiança impostas pelo mercado durante os processos de transformação digital, como já tivemos oportunidade de salientar? E qual deverá ser o papel das entidades públicas, isto é, do Estado? Deverá o Governo estimular o desenvolvimento da economia digital assumindo que cabe às empresas a mitigação dos riscos decorrentes da transformação digital? Ou deverá o Governo desempenhar um papel mais interventivo do que apenas o da sensibilização e de legislador, por via da sanção? Deve o Governo, também por via de incentivos ou instrumentos disponíveis para a transformação digital, assegurar que as empresas tenham, para além das questões relacionadas com tecnologia, também as condições essenciais para acompanhar a sua digitalização com preocupações de nível funcional? Afinal, perante cenários de vantagens e constrangimentos, mais ou menos quantificáveis, resultantes da transformação digital e, em especial, da economia digital, qual deve ser o papel do Governo e das políticas públicas?

Independentemente da pergunta de partida que definimos, sabíamos de antemão que durante o exercício de resposta seriamos confrontados com outras perguntas pelo que definimos que não nos absteríamos, ainda assim, e sempre que possível, de procurar respostas. Neste ponto tornou-se claro que uma tentativa de resposta a algumas das questões que colocámos em cima teria de passar primeiro, e necessariamente, pela compreensão das implicações da transformação digital.

I.3. As implicações da transformação digital

Até aqui tentámos descrever o quadro de desenvolvimento tecnológico em termos gerais e o enquadramento de estímulos e incentivos, políticos e financeiros, em que ele se insere, tanto ao nível europeu como ao nível nacional. Trouxemos ainda para este quadro indícios sobre possíveis impactos ao nível económico, não ignorando, ainda que sem as explorar neste trabalho, as consequentes repercussões ao nível social. Mas, ao certo, de que falamos quando nos referimos à transformação digital nas empresas e que implicações dela decorrem? Nesta secção do nosso trabalho, tentaremos desenvolver um exercício de resposta a esta pergunta.

A transformação digital, que recebeu um enorme contributo por via da mais recente revolução industrial, conforme abordámos em cima, em especial ao nível das comunicações, a Internet, e das TIC, mesmo que apresente ainda alguma indefinição ao nível das suas diferentes fases, compreende, em Gray e Rumpe (2017), dois conceitos conhecidos: transformação e digital. Se por transformação podemos entender um "processo geral que parte de uma situação inicial e que se desloca em direção a uma situação alterada, supostamente melhor", ainda que os autores reconheçam que a escolha de este termo não tenha sido a melhor pelo facto de que as alterações e transformações subjacentes ao

[41] Sobre estratégias de nível funcional nas empresas e as suas diversas áreas funcionais ver Mações, 2017: 64-68.

conceito se verificam de forma contínua não tendo em vista um término, o digital "sugere que muitas das mudanças na sociedade, nos negócios e na indústria serão impulsionadas por tecnologias de informação que permitem que os dados sejam processados em tempo real e até usados para derivar informações de forma inteligente para fornecer às partes interessadas um conhecimento aprimorado sobre os seus processos e produtos" (Gray e Rumpe, 2017: 307).

Nesta linha, cremos poder aceitar-se que a noção de transformação digital se refere "ao processo global acelerado de adaptação técnica por indivíduos, empresas, sociedades e nações em resultado da digitalização" (Khan, 2016: 7). Analisando este processo à luz das empresas, poderemos inferir que a transformação digital destas ocorre com a alteração e adaptação interna do seu funcionamento, em função do paradigma tecnológico, com um expectável impacto externo. Deve, no entanto, assumir-se que esta transformação das empresas é impulsionada não apenas pelo fator tecnológico, e a consequente digitalização, mas em grande medida pela natureza própria das empresas, considerando que estas, como organizações, possuem

> uma estrutura e um sistema de formalização de procedimentos e formas de atuação, um conjunto de formas de organizar e gerir os objetivos organizacionais, as motivações e expetativas individuais, bem como as características contextuais como a dimensão, o poder, a idade e a tecnologia. Esta constitui uma parte de um sistema maior, com o qual interage e cria relações de interdependência. Não é um sistema autónomo, pois que o seu funcionamento e evolução são condicionados por outros componentes do sistema (Ferreira, *et al.*, 2001: xxxi).

Ou seja, pelos ambientes e dimensões envolventes às empresas – "física, tecnológica, económica, políticas, cultural, etc." (Petit e Dubois, 1998: 16) – esta alteração e adaptação às tecnologias, em especial as relacionadas com o digital, "envolve frequentemente transformações nas principais operações comerciais e afeta produtos e processos, bem como as estruturas organizacionais e conceitos de gestão" (Matt, *et al.*, 2015: 339).

Mesmo que as empresas olhem a transformação digital como algo que acrescenta disrupção nas empresas (Nextvalue e CIONET, 2016: 5), dada a multiplicidade de variáveis que afeta, deve referir-se que a digitalização não representa uma panaceia para os problemas ao nível da prestação das empresas: "apesar de existir um estrito consenso na literatura de que a digitalização tem efeitos positivos no crescimento económico, produtividade e bem-estar […], evidências ao nível da digitalização das empresas apontam para que por si só não transformem uma empresa com fraca performance numa de elevada performance dentro do seu setor" (Heinrich, 2014: 182). Acresce ainda o facto de se reconhecer que "os efeitos reais da transformação digital, tanto em termos de resultados disruptivos como de retorno dos investimentos, ainda não são visíveis" (Nextvalue e CIONET, 2016: 5).

Convém também salientar que a discussão em torno da conceção da transformação digital das empresas apresenta duas correntes teóricas: uma que defende que esta transformação das empresas decorre do efeito de estratégias integradas com a sua informatização, isto é, da implementação de medidas que visem a digitalização de infraestruturas da empresa de forma integrada com outras áreas funcionais, por forma a existir uma evolução progressiva do processo de transformação digital; e uma

outra, mais isolacionista, que defende que a transformação digital da empresa assenta exclusivamente em estratégias de informatização da empresa, sem qualquer correlação com as outras áreas funcionais (Hess, *et al.*, 2016). Aquela que aqui se refere vai muito para além das estratégias de informatização das empresas uma vez que estas "habitualmente se focam na gestão de infraestruturas de TI dentro das empresas, com um impacto bastante limitado na tendência das inovações no desenvolvimento do negócio" (Matt, *et al.*, 2015: 339).

Reconhecendo que apesar de acrescentar "e melhorar a capacidade para colaborar e resolver problemas, a tecnologia também acrescenta complexidade e reduz a produtividade em determinados contextos" (Earley, 2015: 58) e as características das empresas e a forma como estas se relacionam, interna e externamente, com o meio envolvente, independentemente do setor em que atuam, a implementação de uma estratégia de transformação digital, segundo Matt, *et al.*, deverá atender a dimensões como a utilização das tecnologias, as alterações na criação de valor, as alterações estruturais e, ainda, os aspetos financeiros (2015: 340).

Não querendo nós apresentar esta como a abordagem estrita a ser adotada pelas empresas, dado que também aqui se encontra uma diversidade de abordagens possíveis à transformação digital, uma vez que estas podem variar em medida, abrangência e escala, consideramos interessante reproduzir aqui um quadro baseado em Hess, *et al*. onde são desenvolvidas algumas questões consideradas chave no momento da decisão de uma empresa avançar com uma estratégia de transformação digital (quadro 1.1).

Quadro 1.1 – Dimensões da transformação digital

Dimensões da Transformação Digital	**Questões base no momento da decisão**
Utilização das tecnologias	• Qual o papel que as TIC desempenham para os objetivos estratégicos da empresa? • Qual a ambição tecnológica para a empresa na abordagem à transformação digital?
Alterações na criação de valor	• Qual o grau de diversidade digital na interação com os clientes da empresa? • Quais serão as fontes de receitas decorrentes da atividade operacional futura da empresa? • Qual o âmbito futuro dos negócios da empresa?
Alterações estruturais	• Quem tem a responsabilidade pela estratégia de transformação digital? • Como serão enquadradas na estrutura organizacional as novas atividades? • Que tipo de alterações operacionais é esperado no futuro? • Que competências serão necessárias e como serão adquiridas?
Aspetos financeiros	• Qual a pressão financeira sobre a atual atividade (negócio) principal da empresa? • Qual a fonte de financiamento para desenvolver a transformação digital e as (novas) atividades que lhe estão associadas?

Legenda: Questões de base no momento da decisão sobre a estratégia de transformação digital das empresas, considerando as várias dimensões dessa transformação digital (fonte: Hess, et al., 2016).

Não obstante, como já aqui aludimos, a dificuldade de medição do impacto da transformação digital e, por conseguinte, da economia digital na economia nacional ou global, é com facilidade que se encontra, na literatura disponível, seja ela dirigida a investigadores, decisores públicos, entusiastas da tecnologia ou ao cidadão comum, um conjunto de referências às vantagens que a transformação digital transporta para as empresas (Bower e Christensen, 1995; MSI, 1997; Lopes, 2001; Salavisa Lança, *et al.*, 2004; 2005; Anderson e Moore, 2006; Anderson, 2007; Pintér, 2008; Moore, 2010; OCDE, 2010; 2012; 2014; 2015; 2017; 2017a; 2017b; A.A.K., 2013; Cerf, 2013; Downes e Nunes, 2013; Schmidt, 2013; Earley, 2014; Harvard Business Review, 2014; Heinrich, 2014; Mazzucato, 2014; World Economic Forum, 2014; Christensen, *et al.*, 2015; Comissão Europeia, 2015; 2016; 2016a; COMPETE 2020, 2015; 2015a; EPRS, 2015; Matt, *et al.*; 2015; Baller, *et al*., 2016; Hess, *et al*., 2016; Jorgenson e Vu, 2016; Rifkin, 2016; Ross, 2016; Franklin, 2017; Gray e Rumpe, 2017; Isaías, *et al*., 2017; Meffet e Mendonça, 2017; Ruan, 2017; Schwab, 2017; 2017a; UNCTAD, 2017).

Mas é também possível a identificação de riscos para as empresas (OCDE, 2008; 2012a; 2015a; Comissão Europeia, 2009; 2012; 2013; 2017; 2017a; Kim, *et al*., 2010; Sommer e Brown, 2011; ENISA, 2012; 2017; 2017a; 2018; Glenny, 2011; Cerf, 2013; Heinrich, 2014; World Economic Forum, 2014; 2016; Angwin, 2015; Hackett, 2015; Hern e Gibbs, 2015; Nunes, 2015; 2016; Rosenquist, 2015; Rotenberg, *et al.*, 2015; Schneier, 2015; EY, 2016; JOUE, 2016a; MARSH, 2016; Canadian Institute of Actuaries, 2017; Cisco, 2017; Newcomer, 2017; Rettman, 2017; Thomas, *et al*., 2017).

De forma sumária, e reconhecendo que estas variam de empresa para empresa, ou mesmo de setor para setor, as potenciais vantagens e riscos percecionados podem ser representados, de forma não exaustiva, como no quadro 1.2.

Quadro 1.2 – Potenciais vantagens e riscos da transformação digital nas empresas

Potenciais vantagens da transformação digital para as empresas	
• Redução de custos de produção; • Maior eficiência nos processos de gestão e de produção[42]; • Mais velocidade na operação das empresas; • Novos modelos de negócio; • Novos produtos e serviços;	• Abertura a novos mercados; • Melhor conhecimento dos mercados e maior interação com fornecedores e clientes; • Melhor alinhamento das necessidades dos clientes com a oferta das empresas; • Maior qualidade na oferta de produtos e serviços.
Potenciais riscos da transformação digital para as empresas	
• Maior concorrência de mercado; • Limitações ao nível das competências (digitais) dos trabalhadores; • Maior exposição ao risco de segurança digital decorrente de ações intencionais e não intencionais (e.g. roubo de informação, disrupção da atividade, dano de reputação[43], etc.); • Barreiras e obstáculos decorrentes de aspetos culturais e estruturais das organizações na implementação da estratégia de transformação digital;	• Digitalização de produtos, serviços e processos sem avaliação de impacto no negócio ou com uma avaliação do impacto inadaptada (múltiplos e sequenciais possíveis pontos de falha devido às interligações, internas e externas, que a transformação digital acrescenta às organizações) – neste ponto destaca-se, principalmente, o impacto que poderá ter a inexistência de uma avaliação dos riscos de segurança digital ou, existindo, uma avaliação dos riscos de segurança digital descontextualizada da realidade tecnológica.

Ainda como evidência da pressão que é colocada nas TIC e na transformação digital como base do desenvolvimento económico e social, aos exemplos de estratégias e políticas públicas que considerámos para este trabalho, poder-se-á considerar outro atribuindo-lhe, provavelmente, o caráter

[42] Importa realçar que, independentemente de se considerar existirem condições para uma maior eficiência nestes processos, não é certa a existência de uma relação causal desta com a produtividade (Evangelista *et al.*, 2014; Earley, 2014).

[43] Para além dos danos de reputação para as empresas como os que já aqui aludimos, isto é, aqueles que resultam da perda de informação, seja relativa aos seus produtos ou aos seus clientes, ou da interrupção dos seus serviços, deve atender-se ao facto da Internet retirar muito do controlo que antes as empresas tinham sobre a informação dos seus serviços e produtos. Atualmente, a facilidade na criação de conteúdos na Internet e a facilidade de disseminação à escala global permite que as empresas sejam mais facilmente atingidas pela crítica e/ou opinião negativa de clientes ou do público em geral, seja pela qualidade dos produtos e/ou serviços que prestam, seja pela qualidade da relação com os clientes ou mesmo pela sua relação com a sociedade.

de expoente mais elevado em termos políticos. Ao mais alto nível internacional, dada a representação de 193 países, os Sustainable Development Goals da ONU[44], com o ano 2030 como horizonte, encara a transformação digital como um meio primordial para a correção das assimetrias e eliminação das barreiras e hiatos entre países, contribuindo para o desenvolvimento social e económico das populações. Nestes objetivos, as TIC desempenham um papel central na sua implementação e sustentabilidade, em matérias que respeitam a educação, saúde e bem-estar, acesso à água e a condições sanitárias, crescimento social e económico, produção e consumo responsável e redução das desigualdades[45].

I.4. As PME e a Cibersegurança

É no quadro anteriormente descrito que o nosso estudo ganha sentido. O impacto que a transformação digital provoca ao nível social e económico, muitas vezes difícil de quantificar, apesar de todas as tentativas para o fazer, deixa percecionar melhor a sua dimensão quando observado qualitativamente. Será essa a nossa abordagem.

Com a tendência global para a digitalização em todas as áreas da sociedade, independentemente das assimetrias locais, regionais e globais, importa não só dar atenção aos aspetos positivos da transformação digital mas, e principalmente, aos aspetos negativos que esta pode introduzir na sociedade, em especial naquele que é comummente considerado o motor da economia, isto é, nas empresas. Importa esclarecer que uma atenção centrada essencialmente nos riscos que a transformação digital possa representar para as organizações, o que inclui empresas, e consequentemente para a economia, não deve ser entendida como sendo um posicionamento cético ou negador da existência de vantagens ou potencialidades da transformação digital. Este foco representa, sim, uma oportunidade para permitir identificar fragilidades e encontrar as melhores soluções para uma tomada de decisão informada: "os desafios são muito diferentes para quem toma decisões no Governo e para quem as toma nos negócios. Mas para ambos é indispensável compreender a sociedade em que agora vão ter de funcionar" (Drucker, 2015: 12). Será este o nosso principal objetivo.

Assim, tendo por pano de fundo os potenciais riscos da transformação digital para as empresas, nomeadamente aqueles que resultam da vulnerabilidade das empresas a ataques intencionais e não intencionais, resultando em eventual roubo de informação, disrupção da atividade, dano na reputação, etc. (ver Quadro 1.2), este estudo partiu da interrogação sobre "como estão as empresas portuguesas, em especial as PME, a lidar com os riscos de cibersegurança e que papel desempenha o Estado, ao nível das políticas públicas, nessa ação". Porque rapidamente constatámos que são poucos os trabalhos focados exclusivamente no setor empresarial português[46] que pudessem permitir verificar

[44] Cf. https://sustainabledevelopment.un.org/sdgs.

[45] Cf. http://close-the-gap.org/the-role-of-ict-in-the-un-sustainable-development-goals/.

[46] Os diversos estudos e trabalhos disponíveis atualmente, que tentam identificar a perceção das empresas relativamente aos riscos ou até sobre o fator de preparação para a sua mitigação, resultam de inquéritos realizados a nível internacional que nem sempre incluem Portugal. Como mais adiante daremos conta, foram

como as empresas, e, uma vez mais, em particular as PME, estão a percecionar e a avaliar os riscos, assim como a implementar medidas, resultantes ou não de eventuais políticas públicas nesta área, fomos forçados a reformular a nossa pergunta de partida. Assim, pela dimensão que implicaria lançar as bases para um trabalho dessa natureza, que não cabe neste e não deixa de propiciar área de investigação para o futuro, focar-nos-emos em quadros teóricos, estudos e inquéritos nacionais e internacionais existentes por forma a desenvolver o nosso estudo com vista a encontrar orientações passíveis de serem adotadas por empresas. Ou seja, tentaremos encontrar respostas para a pergunta "como poderão as empresas portuguesas, em especial as PME, lidar com os riscos de cibersegurança e, face ao quadro de políticas públicas nacional e internacional, que instrumentos têm ao seu dispor para tal?".

Pretendemos, por isso, e com base na bibliografia disponível e acessível em diversas fontes, com recurso à análise do quadro de políticas públicas existente, tentar compreender o papel que desempenha cada ator, e a sua responsabilidade, em particular os atores estatais e as empresas, e detetar eventuais lacunas, assim como possíveis caminhos ainda por percorrer, com o objetivo de identificar orientações possíveis na área da segurança para o digital, comummente denominada por cibersegurança.

O nosso foco nas PME resulta do facto de estas comporem a larga maioria do setor empresarial português, como descrevemos antes, e que não deixa de refletir um pouco a mesma ordem à escala europeia. Ou seja, tal como em Portugal, as PME representam cerca de 99% das empresas na Europa (Paulsen, 2016). Este foco ganha maior pertinência se, a essa evidência, acrescentarmos o facto de que "em cada ano que passa, não só aumenta o volume de ameaças, como também o cenário de ameaças se torna mais diversificado" (Symantec, 2018: 5), partindo do pressuposto de que as PME são mais vulneráveis (Paulsen, 2016), de que estas não estão cientes de como se podem proteger dos riscos a que estão expostas (RSA, 2016), e de que estas se tornaram alvo preferencial de atacantes por disporem de menos recursos para se defenderem quando comparadas com empresas grandes (Daniels, 2017).

Estes pressupostos aparentam contrariar uma lógica de que serão as grandes empresas as que são alvos mais apetecíveis para atacantes e criminosos, dado que, por via do senso comum, são as que disporão de mais recursos financeiros passíveis de ser subtraídos ou explorados, e as que sofrerão maiores prejuízos na eventualidade de um ataque ou exploração de vulnerabilidades. No entanto, dados mostram que, ao longo dos anos, tem-se verificado uma tendência de aumento de ataques a empresas de menor dimensão e uma diminuição dos ataques às grandes empresas (Symantec, 2016; Toesland, 2016). Na base desta constatação podem estar razões como:

- a passagem da utilização de sistemas isolados para a utilização de sistemas interligados em consequência da transformação digital, o que aumenta a exposição das PME aos riscos;

---

poucos os que identificámos, a nível internacional, que consideram o enquadramento ou a realidade portuguesa, assim como os que, a nível nacional, se focam nas empresas portuguesas.

- uma menor preparação para fazer face a ataques dada a diferença na prioridade atribuída à segurança digital em relação à prioridade que habitualmente se encontra nas grandes empresas;
- a maior capacidade que as pequenas empresas vão tendo para armazenar dados e estes poderem representar grande valor económico;
- e também as ligações e relações que se estabelecem entre empresas e mercados, podendo fazer das pequenas empresas portas de entrada para perpetrar ataques em grandes empresas (Toesland, 2016).

Em última análise, mesmo nas situações em que não são o alvo preferencial de atacantes, as PME podem sofrer efeitos colaterais em resultado de ataques lançados de forma alargada, na tentativa de apanhar no seu caminho todas aquelas organizações que se mostrem mais vulneráveis: “Hoje em dia, com todas as empresas a conectarem cada vez mais os seus negócios à Internet, a ameaça é agora universal” (Poppensieker e Riemenschnitter, 2018).

CAPÍTULO II: DADOS E METODOLOGIA

II.1. Ciberespaço, Cibersegurança e Risco de Segurança Digital

À medida em fomos desenvolvendo o nosso quadro teórico, tentámos torná-lo claro com a explicitação dos termos e dos conceitos que foram sendo utilizados, uma situação que resulta de uma opção consciente. Fizemo-lo, sempre recorrendo a autores e a trabalhos – umas vezes fontes primárias e outras a fontes secundárias – que dedicaram alguma atenção a essas temáticas: quando abordámos as revoluções industriais, a transformação digital e a economia digital, a competitividade e a tecnologia, e também as organizações e as empresas. Importa agora fazer o mesmo para os conceitos que acompanharão, agora com mais frequência do que antes, o nosso trabalho, nomeadamente a cibersegurança e risco de segurança digital, mas não sem antes fazermos aqui uma clara destrinça entre "Estado" e "Governo".

Sem invadir o campo da Ciência Política, e não entraremos, por isso, numa dissertação conceptual, sentimos esta necessidade porque frequentemente se misturam os conceitos de Estado e Governo quando se alude à definição e execução de políticas públicas. Partimos, assim, do conceito de Estado como "uma comunidade de pessoas que, a fim de realizar os seus ideais de bem comum, institui num dado território, por autoridade própria, um poder capaz de dirigir a vida coletiva" (Amaral, 2014: 93) ou, de outra forma, "uma realidade social juridicamente organizada num certo espaço físico para a prossecução de fins de interesse geral (bem comum)" (Amaral, 2014: 93). É, portanto, ao segundo – ao Governo – que cabe a direção da administração direta do Estado, a orientação da administração indireta e a fiscalização da administração autónoma (Amaral, 2014: 134-135).

Abstemo-nos ainda de traçar a evolução histórica do conceito de cibersegurança[47], destacando apenas que o mesmo tem sofrido alterações conceptuais ao longo do tempo e, desde a primeira década do século XXI, apesar de não ter uma aplicação consensual, é utilizado transversalmente no dia-a-dia, pelos meios académicos, empresariais e governamentais, em múltiplas situações relacionadas com os aspetos da segurança em ambientes digitais – uma transversalidade que, na ótica de Schatz, *et al.*, sem a devida conceptualização, pode induzir "problemas consideráveis no contexto de estratégia organizacional, objetivos de negócio ou acordos internacionais" (2017: 53). Reconhecem-se também as dificuldades identificadas em algumas tentativas de definição do conceito de cibersegurança, seja pela diversidade de interpretação pelos diversos intervenientes (Klimburg, 2012; Craigen, *et al*., 2014; Schatz, *et al*., 2017), ou porque a investigação nesta matéria assenta, essencialmente, em revisões bibliográficas na língua inglesa, podendo dessa forma ignorar tentativas de definição noutras línguas e porque a própria grafia varia na língua inglesa, uma vez que é possível encontrar referências a "cybersecurity" e "cyber security" obrigando o investigador a uma atenção redobrada aquando da necessidade de recorrer a palavras-chave. No entanto, das múltiplas tentativas de definição do conceito de cibersegurança, destacamos duas passíveis de serem aceites neste trabalho. A primeira, de

[47] Sobre a evolução histórica deste conceito e da terminologia adotada ao longo dos tempos, ver Internet Society, 2012; Craigen, *et al*., 2014; Paulsen, 2016; e Schatz, *et al*., 2017.

Craigen, *et al*., que define cibersegurança como "a organização e coleção de recursos, processos e estruturas utilizadas para proteger o ciberespaço e os sistemas habilitados para o ciberespaço de ocorrências desajustadas entre o *de jure* [de direito] e o *de facto* dos direitos de propriedade"[48] (2016: 17). A segunda, de Schatz, *et al*., apresenta-nos a cibersegurança como

> "a abordagem e as ações associadas aos processos de gestão de risco de segurança seguida pelas organizações e Estados para proteger a confidencialidade, integridade e disponibilidade de dados e bens utilizados no ciberespaço. O conceito inclui orientações, políticas e recolha de salvaguardas, tecnologias, ferramentas e formação para permitir a melhor proteção para o estado do ambiente ciber e dos seus utilizadores" (2017: 66).

Dado que esta segunda definição nos parece ter uma maior abrangência, mesmo acompanhando o reconhecimento de algumas limitações na base da sua conceção (Schatz, 2017: 67), e por a identificarmos com um melhor enquadramento para a Estratégia Nacional de Segurança do Ciberespaço (ENSC), aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, considerando o âmbito atribuído pelo legislador português na sua definição, e da qual falaremos mais adiante, assim como a relação que tem com a mais recente proposta de definição ao nível UE[49], será este o conceito subjacente ao nosso trabalho.

A referência ao conceito de cibersegurança pressupõe a coexistência com um outro conceito, também ele pouco consensual entre autores – académicos e governamentais[50]. Trata-se do conceito de ciberespaço, do qual, habitualmente, "se dispõe sem grande preocupação de exatidão e relativamente ao qual poucos dos que o usam saberia definir o sentido, senão de forma vaga" (Santos e Marques Guedes, 2015: 190). Por essa razão, nas diversas tentativas de definição conceptual de ciberespaço (Strate, 1999 citado em Santos e Marques Guedes, 2015; Klimburg, 2012; Nunes, 2015; 2018; Gouveia e Santos, 2015: 60-63), encontramos um melhor reflexo naquela definida pela International Organisation for Standardisation (ISO): "o ambiente complexo resultante da interação de pessoas, software e

[48] Itálicos no original. Tendo sido a nossa opção, desde o início, apresentar todas as citações traduzidas para a língua adotada na redação deste trabalho, dada a possibilidade de a citação em causa poder suscitar outra tradução para além da nossa interpretação, entendemos apresentá-la aqui na sua versão original: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights."

[49] "[…] entende-se por: «Cibersegurança»: as atividades necessárias para proteger de ciberameaças as redes e dos sistemas de informação, os seus utilizadores e as pessoas afetadas; […] (Comissão Europeia, 2017b: 40).

[50] Consideramos a existência de "autores governamentais", em virtude de, nesta matéria, alguma da bibliografia existente ser produzida por entidades públicas, nomeadamente por Governos, como são as estratégias, legislação ou estudos encomendados.

serviços na Internet através de dispositivos tecnológicos e de redes ligadas a ela, que não existem em qualquer forma física"[51] (Klimburg, 2012: 8).

Num cenário em que o conceito de ciberespaço, "onde assenta a Internet, uma rede global de troca de informação e conhecimento" (Paulo Moniz em Nunes, 2018: 18), e mesmo o de cibersegurança, é utilizado de diversas formas, em diversos contextos e por múltiplos atores, é passível de ser aceite que "genericamente falando, o ciberespaço é um novo meio – ou um conjunto de novos meios – que configura um novo contexto nas relações institucionais, grupais ou individuais, com o potencial e a capacidade para alterar os equilíbrios existentes" (Santos e Marques Guedes, 2015: 191). E é neste "novo meio", ou "conjunto de novos meios", com um enorme potencial de expansão[52], perante a crescente emergência de fatores de risco como ameaças, vulnerabilidades e incidentes, que emergem também preocupações com a proteção e a segurança da informação e dos sistemas. Importa, por isso, para evitar ou mitigar as consequências das ações que possam resultar de incidentes com origem na exploração dessas ameaças e vulnerabilidades, que sejam definidos mecanismos de gestão de riscos de segurança digital. Neste campo, e considerando a sua evolução teórica, muito impulsionada pela OCDE (2015a: 27), o nosso trabalho tem por pressuposto que risco de segurança digital

> "é a expressão utilizada para descrever uma categoria de risco relacionada com o uso, desenvolvimento e gestão do ambiente digital no decurso de qualquer atividade. Este risco pode resultar da combinação de ameaças e vulnerabilidades no ambiente digital. […] O risco de segurança digital é dinâmico por natureza. Inclui aspetos relacionados com os ambientes físicos e digitais, as pessoas envolvidas na atividade e os processos organizacionais que os suportam" (OCDE, 2015a: 30).

Acrescentamos também que ciberataque pode ser genericamente "entendido como uma sequência de ações destinadas a produzir um resultado não autorizado ou uma perturbação indesejada na confidencialidade, na integridade ou na disponibilidade de um serviço ou produto" (Lino Santos em Nunes, 2018: 26).

Porque mais adiante a expressão "cultura de cibersegurança" será utilizada na exposição dos nossos argumentos, importa defini-la antecipadamente. Por cultura de cibersegurança entende-se o

> conhecimento, convicções, perceções, atitudes, suposições, normas e valores pessoais em relação à cibersegurança e como eles se manifestam no comportamento das pessoas com as tecnologias da informação. A cultura de cibersegurança faz com que considerações sobre segurança da informação sejam parte integrante do trabalho, dos hábitos e da conduta dos trabalhadores, integrando-a nas suas ações quotidianas. Adotar a correta abordagem na segurança da informação permite que uma cultura de

[51] Julgamos, uma vez mais, poder ser útil a apresentação da citação na sua versão original: "the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form."

[52] Para maior aprofundamento deste "novo domínio", com uma responsabilidade partilhada e sem fronteiras, e a sua categorização como um "*Global Common*", à "semelhança dos mares, o espaço aéreo e o espaço exterior", e a sua relevância no funcionamento da sociedade, ver Paulo Moniz em Nunes, 2018: 17-19.

> cibersegurança resiliente se desenvolva naturalmente a partir de comportamentos e atitudes dos trabalhadores em relação aos ativos de informação no trabalho, e, como parte da cultura organizacional mais ampla da empresa, a cultura de cibersegurança pode ser moldada, direcionada e transformada. (ENISA, 2017a: 7)

O nosso trabalho apresenta um enorme risco que não queremos deixar de salientar. Um risco que resulta de um único aspeto: a dinâmica tecnológica. Como salientámos, o desenvolvimento de qualquer um destes conceitos foi assente numa dinâmica evolutiva da tecnologia bastante rápida, e que se transferiu, e transfere, para os ambientes envolventes. Por isso, o risco que corremos é o de vermos, em breve, as nossas opções conceptuais ultrapassadas. Não estamos, assim, imunes à constatação de que "faz parte da natureza do conhecimento que ele se altere rapidamente e que as certezas de hoje se transformem em absurdos amanhã" (Drucker, 2015: 70). Esclarecemos, portanto, que as nossas escolhas obedeceram, pelo menos, a três critérios: a de terem pressupostos académicos, a de terem uma aplicabilidade real e ainda a de terem algum reconhecimento internacional.

II.2. Seleção de técnicas

Em termos metodológicos, e reconhecendo desde o início a complexidade inerente a qualquer estudo que tenha como seu objeto o universo das PME e o quadro teórico anteriormente traçado, nomeadamente quando abordámos a economia digital em Portugal, não nos podemos desviar, para este trabalho, da utilização de um método indutivo. Ou seja, dada a dificuldade que prevemos em testar empiricamente quaisquer hipóteses passíveis de serem extraídas do nosso quadro teórico, e seriam algumas, partiremos de observações e de proposições específicas numa tentativa de generalizar o seu enquadramento. Admitimos, assim, um certo nível de incerteza nas nossas conclusões que poderão, eventualmente, contribuir para, ou serem desenvolvidas, em trabalhos futuros.

Cientes da natureza difícil na realização de inquéritos, em especial pelo eventual grau de incerteza que poderiam advir das respostas considerando que, como já referimos antes, alguns aspetos nesta matéria se tornam de particular sensibilidade para algumas empresas[53], ou em tomar como objeto de estudo um setor de atividade específico e assim correr o risco de limitar, ou mesmo anular, uma intenção de correlacionar uma área transversal como é a da cibersegurança ou a do risco de segurança digital com as políticas públicas, foi nossa opção desenvolver este trabalho tendo em conta uma abordagem abrangente de teor qualitativo baseada, essencialmente, em análise documental.

Como forma de reforçar a informação obtida através da análise documental, entendemos realizar entrevistas a atores que se consideraram relevantes nas matérias estudadas. O objetivo destas entrevistas foi o de nos ser possível identificar aspetos que pudessem contrariar ou reforçar a literatura

[53] Este tipo de situações, para além da bibliografia apresentada que constata esta dificuldade, pode ser inferido de questionários realizados nesta área. A título de exemplo, e no caso português, em Cardoso *et al*. (2017) e AP2SI (2016) é possível observar que quando inquiridos sobre deteção e concretização de ataques e incidentes nas organizações, os respondentes optam maioritariamente pela resposta "não sabe" ou "não responde".

identificada à luz da experiência e realidade portuguesa. Nesse sentido, das 12 entrevistas inicialmente previstas, foram concretizadas seis:

- três a peritos e investigadores, que também exercem a atividade de docência em universidades, públicas e privadas, e com os quais foi assumido o anonimato em eventuais citações (Anexo A);
- a um gestor público na área de gestão de incentivos e financiamento, com o qual foi assumido o anonimato em eventuais citações (Anexo C);
- à AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação, uma associação sem fins lucrativos e de natureza privada, com membros individuais e coletivos (Anexo B):
- ao Gabinete Nacional de Segurança (GNS), no qual está integrado e funciona o Centro Nacional de Cibersegurança (CNCS) (Anexo D).

Foram também contactadas associações e confederações representativas das empresas em Portugal sendo que apenas uma, a CIP – Confederação da Indústria Portuguesa, retribuiu o contacto indicando não poder fornecer respostas às questões que havíamos preparado dado que iniciou, muito recentemente, o seu trabalho neste domínio. Face à impossibilidade de obter contributos junto destas organizações representativas do setor privado, equacionámos a realização de entrevistas diretamente a empresas. No entanto, uma vez confrontados com o facto de um eventual contributo resultante destas entrevistas isoladas não poder ser visto como representativo de um setor de atividade ou de uma tipologia de empresa, por forma a evitar que nosso estudo se baseasse em proposições arbitrárias, isto é, baseadas em práticas de empresas determinadas para este exercício, a nossa opção passou por nos basearmos em estudos e trabalhos existentes sobre práticas empresariais relacionadas com a cultura organizacional e a cibersegurança.

Junto de peritos e investigadores, porque também são docentes universitários, tentámos perceber qual a resposta que a academia, designadamente o ensino superior, está a dar aos desafios que emergem da transformação digital e da cibersegurança. A relação deste setor com o setor privado e as políticas públicas foi também um tema para o qual tentámos obter as suas perceções.

Na entrevista com um gestor público na área de gestão de incentivos e financiamento, pretendemos perceber se o sistema nacional de incentivos para a promoção da transformação digital do setor privado compreende também respostas aos desafios que são colocados pelos riscos e ameaças no ciberespaço. Procurámos ainda conhecer a sua perceção sobre a atenção dada por gestores e empresários às questões da cibersegurança no momento da decisão pela digitalização das suas empresas, ou parte delas, bem como saber se considerava adequada a resposta da academia no que respeita à formação de especialistas em TIC e de gestores.

À AP2SI, pela missão que pretende desempenhar, foram dirigidas perguntas com o objetivo de obter a sua perceção e conhecimento sobre os processos de transformação digital das empresas e o envolvimento das áreas funcionais destas. Nas perguntas dirigidas a esta associação foi também

tomado em consideração o “Inquérito Aberto à Segurança da Informação das Instituições em Portugal”, conduzido por esta, e o seu eventual envolvimento em consultas no âmbito dos processos de definição de políticas públicas.

Por fim, com a entrevista ao GNS/CNCS pretendemos analisar em maior profundidade o percurso e os métodos utilizados nos processos de tomada de decisão relacionados com as mais recentes políticas públicas no domínio da cibersegurança. Procurámos também perceber o processo de coordenação político-estratégico que está atribuído àquela organização nesta matéria, bem como o seu envolvimento com os demais setores da sociedade, nomeadamente a sua relação com a academia e o setor privado.

Um tronco comum em todas as entrevistas realizadas foi inquirir sobre a perceção dos entrevistados em relação às vantagens e desvantagens e aos riscos da transformação digital para as organizações, atendendo ao tema da cibersegurança. Não obstante o guião previamente definido para as perguntas, as entrevistas presenciais gozaram da total liberdade dos entrevistados, e também do entrevistador, para abordar questões relacionadas com as respostas que iam sendo fornecidas no decurso das entrevistas.

Outro aspeto que integrou a metodologia adotada neste trabalho foi a observação participante, sendo que neste campo importa darmos conta de uma dificuldade acrescida pelo acesso de que dispomos a documentação classificada ou documentos de trabalho internos, forçando-nos a um exercício permanente e redobrado de seleção da informação, assim como o de manter omissa toda e qualquer informação classificada com, certamente, algum prejuízo para este trabalho dada a sua relevância e valor que lhe poderia acrescentar.

Aproveitando a flexibilidade de análise inerente ao método qualitativo, o nosso trabalho procura, essencialmente, descrever e explicar relações, experiências ou normas, por forma a poder ser encarado como um instrumento para a compreensão do enquadramento destas matérias com as políticas públicas, numa modesta ambição de se constituir como um contributo entre muitos para uma tomada de decisão mais informada.

II.3. Recolha de dados

Como já aqui foi mencionado, os trabalhos disponíveis sobre o quadro português relativamente à abordagem das empresas às questões de cibersegurança, nomeadamente trabalhos que indiciem ou avaliem a existência de uma cultura de cibersegurança nas empresas, e em especial nas PME, são verdadeiramente escassos. Naqueles que existem, com metodologias e abordagens diferentes, e nem sempre com uma periodicidade que permita a construção de um histórico neste campo, e muito longe da já referida necessidade “da institucionalização de um sistema de avaliação no nosso país” (Lopes, 2013: 10), encontram-se trabalhos desenvolvidos por organizações do setor privado, mais na vertente de avaliação da perceção dos riscos e de continuidade de negócio nas organizações (KPMG, 2018; MARSH, 2016; 2017), por associações de profissionais, com o objetivo de contribuir para traçar um quadro de referência sobre a realidade nacional (AP2SI, 2016), ou, de forma exploratória, pela

academia (Cardoso, *et al.*, 2017). Com base em dados recolhidos nestas fontes, confrontando-os com outros que traçam o quadro internacional (WEF, 2014; EY, 2016; MARSH, 2016; RSA, 2016; Canadian Institute of Actuaries, 2017; Carrapico e Barrinha, 2017; Cisco, 2017; ENISA, 2017; Symantec, 2018) e conjugando-os com trabalhos que apontam para explicações da perceção sobre políticas públicas em matéria de cibersegurança (Correia, *et al.* 2016; 2017; ENISA, 2017a), julgamos ainda assim ser possível estabelecer um contributo relevante para uma discussão necessária em Portugal em torno da criação de bases para o estabelecimento de uma cultura de cibersegurança nas empresas. Este contributo sai altamente beneficiado pelas entrevistas, mencionadas anteriormente, levadas a cabo a entidades de relevo nestas matérias.

CAPÍTULO III: RESULTADOS E DISCUSSÃO

III.1. As ameaças

Podemos, agora, com algum grau de certeza e sustentação teórica e empírica constatar que:

i. Está em curso um processo, dificilmente travado, de transformação digital;

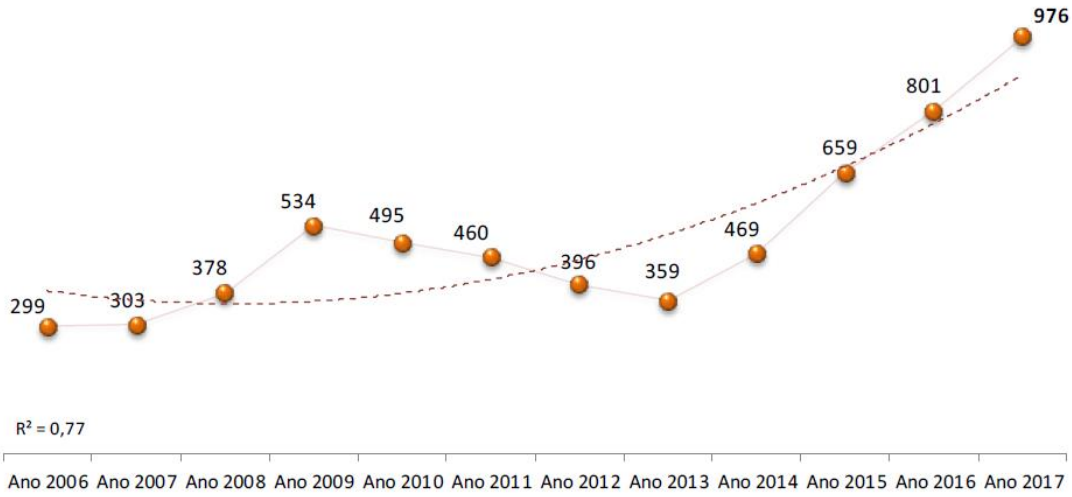
ii. Este processo, alicerçado na inovação tecnológica fortemente alimentada pelo desenvolvimento científico e associado ao fenómeno da globalização, está a introduzir profundos impactos, positivos e negativos, na sociedade e na economia, e, por conseguinte, nas organizações, incluindo as empresas;

iii. A dinâmica da transformação digital nas organizações, em especial nas empresas, é em grande medida promovida por incentivos diretos – políticos e financeiros – e indiretos – vantagens económicas, concorrência, eficiência, imagem, etc.;

iv. Estes incentivos, formais e informais, deixaram de ter no plano nacional a sua fonte de estímulos e passaram a tê-la, também, nos planos europeu e internacional.

Através do Relatório Anual de Segurança Interna (RASI) 2017, que em Bernardo é caracterizado como "pobre em construções causais, é um compêndio de dados agregados" (2018: 9), é possível verificar um aumento de cerca de 21,9% do número de participações de crimes informáticos em Portugal (Sistema de Segurança Interna, 2018). Chamamos desde já a atenção que, por este indicador considerar tipologias como "acesso indevido ou ilegítimo/interceção ilegítima, falsidade informática, outros crimes informáticos, reprodução ilegítima de programa protegido, sabotagem informática, viciação ou destruição de danos/dano relativo a dados/programas" (Sistema de Segurança Interna, 2018: 32), reveste-se de enorme dificuldade a tentativa de fazer uma extrapolação de valores para um quadro afeto exclusivamente a organizações ou a empresas dado que alguns destes crimes podem igualmente ser perpetrados contra pessoas singulares. Ou seja, a informação disponibilizada publicamente não nos permite aferir em que grau os crimes informáticos afetam, ou afetaram, as empresas em Portugal. Este Relatório salienta também que "quanto à criminalidade informática e praticada com recurso a tecnologia informática verifica-se um aumento generalizado, destacando-se o crime de acesso ilegítimo ou indevido, devassa por meio informático, falsidade informática e a sabotagem informática, com variações crescentes, respetivamente, 21%, 16%, 16% e 27% em relação ao ano transato" (Sistema de Segurança Interna, 2018: 31).

Figura 3.1 – Participações de crimes informáticos em Portugal



Legenda: gráfico com a evolução do número de participações de crimes informáticos em Portugal (fonte: Sistema de Segurança Interna, 2018)

Ainda que sem uma sustentação argumentativa que permita compreender as suas causas, o mesmo Relatório prevê um aumento das situações passíveis de constituir ilícitos nesta área, projetando

> uma previsão de aumento dos seguintes *modi operandi*: APT (*advanced persistent threat*): interligação de *botnets* e *malware* bancário; branqueamento de capitais com recurso a moedas, contas bancárias e cartões virtuais; conhecimento de exfiltração de informação sensível; acessos ilegítimos sobre alvos predefinidos; exposição a campanhas de extorsão com base em programas maliciosos (*ransomware* e extorsão *sextortion*) (Sistema de Segurança Interna, 2018: 31).

Prevê igualmente o "aumento de anonimização na navegação e cifragem de dados, com a correspondente insuficiência do Estado para a decifragem, afetando a prevenção e a recolha de informação e de prova"54 (Sistema de Segurança Interna, 2018: 31).

[54] Não tendo este trabalho espaço para fazer eco dessa discussão, existe a nível internacional um debate, com mais de 20 anos (Terceiro, 1997: 198-200), em torno do mesmo argumento utilizado neste Relatório, ainda que sem referências causais, sobre a "insuficiência do Estado para a decifragem" de comunicações ou aplicações para efeitos de "prevenção e a recolha de informação e de prova". Este debate internacional centra-se em questões técnicas, éticas, sociológicas e até económicas, sendo um dos argumentos da comunidade técnica o do que a via que permite às autoridades judiciárias – responsáveis pela investigação – desenvolver ações de monitorização e recolha de informação é a mesma que permite o acesso a agentes que têm intenção de perpetrar atos criminosos, e que a referida insuficiência do Estado resulta de uma menor aposta na referida prevenção e investigação por via orçamental, técnica e de recursos humanos. Sobre as questões de privacidade, vigilância e segurança, cf. Landau, 2013; Angwin, 2015; Rotenberg, *et al*., 2015; Donohue, 2016. Esta discussão voltou a ganhar alguma visibilidade mediática em 2016 com o caso "Apple vs. FBI", disputado em tribunais nos

Neste ponto, conceptualmente, "sextortion" é definido pela INTERPOL como chantagem em que informação ou imagens de cariz sexual são utilizadas para extorquir às vitimas favores sexuais e/ou dinheiro[55]. Relativamente aos outros conceitos mencionados, seguimos aqui as definições apresentadas pela ENISA:

- "botnet" refere-se a "um conjunto de computadores infetados por bots", sendo um bot "um software malicioso" controlado centralmente por outro computador[56];
- "malware" tem origem na expressão "Malicious Software" e trata-se de um software, ou parte dele, que executa operações não desejadas ou solicitadas, tais como roubo de dados ou qualquer outra que possa comprometer computadores[57];
- "ransomeware" trata-se de um tipo de "malware" que infeta sistemas de computadores de utilizadores manipulando-os para que as vítimas não consigam, parcialmente ou completamente, utilizar os computadores sendo, normalmente, alvo de chantagem para efetuarem pagamentos de dinheiro para poderem voltar a aceder aos sistemas e ficheiros[58].

Das ATP identificadas no RASI 2017, são estas últimas as ameaças que habitualmente são utilizadas para prejudicar ou obter vantagem sobre as organizações, em especial as empresas. Destas pode destacar-se os ransomware com uma tendência crescente ao longo dos últimos anos (Symantec, 2016; 2017; Europol, 2018). Mesmo ocupando o sétimo lugar no cenário das 15 maiores ameaças no ciberespaço, traçado pela ENISA para o ano de 2017, observa-se esta tendência de crescimento em relação a 2016 (ENISA, 2018a: 9), apresentando-se como uma exploração de vulnerabilidades rentável junto de pessoas e organizações: "a sua rentabilidade não só permaneceu elevada, como continuou a crescer" (ENISA, 2018a: 55). Deve, no entanto, salientar-se que, apesar de definir o ransomware como um tipo de malware, a ENISA apresenta estes dois tipos de ameaças de forma separada, encontrando-se o malware posicionado na primeira posição das 15 maiores ameaças no ciberespaço.

Mas se as ameaças são amplamente conhecidas, as razões e motivações por detrás dos incidentes e ataques podem variar e são, muitas vezes, desconhecidas. Sendo este um aspeto cujo conhecimento se revela de elevada importância para a implementação de mecanismos de proteção e de respostas a dar em caso de incidentes e ataques, baseando-nos na bibliografia disponível,

---

EUA, em que o segundo exigia que a primeira fornecesse mecanismos de acesso a informação cifrada nos dispositivos que fabrica (cf. https://www.nytimes.com/news-event/apple-fbi-case, consultado em 28 de junho 2017).

[55] Em https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion, consultado em 13 de junho 2018.

[56] Em https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets, consultado em 13 de junho 2018.

[57] Em https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware, consultado em 13 de junho 2018.

[58] Em https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware, consultado em 13 de junho 2018.

apresentamos resumidamente no quadro seguinte as principais razões e motivações, bem como algumas das suas características, que estão na origem de incidentes e de ataques a organizações, incluindo as empresas, através do ciberespaço (quadro 3.1).

Quadro 3.1 – Razões e motivações na origem de incidentes e ataques a organizações através do ciberespaço

Razões e Motivações	**Características**
Motivações financeiras	Os crimes com vista à obtenção de vantagens financeiras são, habitualmente, dirigidos a alvos específicos, ou identificados em ações massificadas, para recolher informações e acessos pessoais através de endereços de internet e informações falsas, tentado fazer-se passar por entidades reais (phishing). Para além da ação de criminosos de forma isolada, têm surgido dados que indiciam a existência de redes organizadas para perpetrar este tipo de crimes. Frequentemente estes crimes visam a fraude, roubo ou extorsão.
"Hacktivismo"	Considerar-se "hacktivistas" aqueles que encetam ataques através do ciberespaço com motivações políticas, sociais, ambientais, etc., sendo os alvos preferenciais organizações públicas e privadas. Estes ataques podem implicar a negação de serviços ou a alteração da imagem das organizações visadas, bem como o roubo de dados. Não é comum identificarem-se motivações financeiras associadas a este tipo de iniciativas.
Subversão	As razões desta categoria de ataques e exploração de vulnerabilidades estão, muitas vezes, associadas ao "hactivistmo". Os ataques podem igualmente ser dirigidos a organizações públicas e privadas.
Religião ou nacionalismo	Nesta categoria são, habitualmente, identificados indivíduos e organizações que se intitulam de "ciberguerreiros" tendo por base razões religiosas ou ideologias normalmente associadas ao patriotismo ou nacionalismo extremos.
Terrorismo	À semelhança da categoria anterior, com a intenção de provocar medo e ataques de dimensão considerável, encontram-se indivíduos e organizações, normalmente de forma coordenada, com múltiplas motivações, entre as quais a religião ou o nacionalismo. Em alguns casos, estas ações incluem motivações financeiras.
Desafio	A tentativa de desafiar ou de superar sistemas de proteção e segurança são razões que levam indivíduos, habitualmente de forma isolada, a efetuar ataques de diversa natureza no ciberespaço contra organizações. É possível encontrar referências que denominam esta

	motivação como “script kiddies”.
Notoriedade	Muitas vezes associado ao desafio e à superação dos sistemas de proteção e segurança está, também, o desejo de ser conhecido. A tentativa de conquistar um grau de respeito dentro das comunidades hackers ou das comunidades da cibersegurança costuma estar, igualmente, associado a estes ataques.
Vingança	A vingança contra pessoas ou organizações é uma das razões de ataques ou roubo de informação que, algumas vezes, quando se trata de organizações ou empresas, podem ser perpetrados por pessoas internas, isto é, que, por alguma razão, por forma a se vingarem, obtêm indevidamente, expõem ou danificam informação ou infraestruturas das organizações a que pertencem ou pertenciam.
Espionagem	A exploração de vulnerabilidades motivada por espionagem pode ocorrer de diversas formas (phishing, malware, agentes internos, entre muitas outras) e, não descartando organizações sem fins lucrativos ou de caráter social, é essencialmente dirigida a organizações dos setores público e privado. Estados e empresas são alvos altamente apetecíveis para estes atores dadas as vantagens políticas, estratégicas, concorrenciais e financeiras que poderão advir da informação obtida por via de ataques informáticos ou exploração de vulnerabilidades. Estas razões e motivações podem estar na origem da ação não só de indivíduos ou redes organizadas de indivíduos, mas também dos próprios Estados visando outros Estados ou empresas localizadas em outros Estados, e ainda de empresas contra empresas concorrentes.

Legenda: Quadro resumo das razões e motivações para os incidentes e ataques às organizações através do ciberespaço resultante da bibliografia consultada (fontes: Mathews, 2016; Symantec, 2016; 2017; Bailey, et al., 2018; Europol, 2018)

Este quadro permite-nos perceber que, para além das múltiplas ameaças a que as organizações podem estar expostas, as razões e os atores na sua origem podem ser igualmente múltiplos. Mas não deve julgar-se que a exploração de vulnerabilidades ou os ataques dirigidos às organizações terão uma única motivação. Eles podem, em alguns casos, compreender simultaneamente várias finalidades e utilizar vários métodos e formas para as atingir. Não obstante a dependência técnica e tecnológica para a concretização destas atividades, a ação dos autores destas ações tem, também ela, subjacente o fator humano. Há, por isso, uma tendência para olhar para estas ameaças e as suas razões numa perspetiva que as classifica de ações oportunistas, onde os autores podem ser criativos mas, pela ausência de planeamento, podem ver-se confrontados com momentos de frustração e, consequentemente, erros que poderão levar à sua exposição; de ações de multidão, onde o autor acompanha de forma emocional e pouco disciplinada, por vezes sem um objetivo claramente definido,

um movimento criado; e ainda ações onde a determinação está muito presente no planeamento e na assertividade com que determina o seu objetivo (CIONET, 2015).

Não deve, no entanto, e independentemente das razões ou motivações, julgar-se que estas ameaças são exclusivamente externas. Para além das ameaças externas que as organizações devem atender, devem igualmente estar preparadas para lidar e enfrentar ameaças internas. Numa análise conduzida pela McKinsey a milhares de violações de informação e incidentes publicamente reportados, foi possível constatar e identificar que a componente interna esteve presente em cerca de 50% dessas situações (Bailey, *et al.*, 2018). Da mesma forma, para além das intenções maliciosas, deve atender-se a que os incidentes podem igualmente resultar de ações de negligência ou de cooptação de pessoas internas por parte de atores externos. No mesmo trabalho conduzido pela McKinsey, verificou-se que estas ações estiveram presentes em cerca de 44% dos casos analisados (Bailey, *et al.*, 2018).

Todos estes são aspetos que devem condicionar e determinar a ação e preparação das organizações, sejam elas públicas ou privadas, perante os riscos de exposição decorrentes do processo de transformação digital.

III.2. As organizações e as empresas

A análise de alguns trabalhos disponíveis indicia a existência por parte das organizações – empresariais e não empresariais – de alguma perceção crescente dos riscos atuais e futuros inerentes aos ambientes digitais, ainda que de uma forma geral e abstrata.

Ao nível da perceção das empresas, o risco de "ataques terroristas em larga escala" a nível mundial ocupava, em 2016 e 2017, o primeiro lugar no leque de preocupações e foi substituído, em 2018, pelo risco de "ataques cibernéticos em grande escala". Já a preocupação das empresas com a "instabilidade política ou social" em Portugal, em 2016 e 2017, foi ultrapassada em 2018 pela preocupação com "ataques cibernéticos" (MARSH, 2018: 8). Esta aparente crescente preocupação com os ciberataques parece ser uma tendência no panorama internacional, uma vez que, conforme identifica o WEF, este é um risco que, em 2018, voltou a figurar na lista dos cinco principais riscos[59], ocupando o terceiro lugar daqueles cuja perceção aponta uma forte probabilidade desse fenómeno acontecer a nível global (WEF, 2018: 14-16).

Um dos problemas já aqui identificados, o que parece reforçar a importância da realização de inquéritos e o aprofundamento de estudos nestas matérias, é o facto dos trabalhos neste domínio, e também em Portugal, nem sempre considerarem uma segmentação por tipo de organização. Isto é, em boa parte destes trabalhos é comum encontrar-se, quase sempre, uma apresentação de resultados onde são agregadas empresas com entidades públicas e com organizações privadas sem fins

[59] Segundo o mesmo relatório do WEF de 2018, o risco de ciberataques constou neste grupo de cinco principais riscos globais em 2012 no quarto lugar e em 2014 no quinto lugar. Refira-se ainda, e estabelecendo uma correlação com as questões do ciberespaço, uma subida de posição do risco de fraude ou roubo de dados em massa.

lucrativos. Nesse sentido, vemo-nos forçados à utilização da expressão "organizações" sem fazer, como seria a nossa intenção, a devida distinção por tipologia, salvo nas situações devidamente assinaladas.

Um outro aspeto que reforça a importância de serem desenvolvidos mais trabalhos nesta área é o facto de eles poderem contribuir para responder a uma necessidade de mais sensibilização para as questões da cibersegurança, seja para as organizações, empresas ou não, seja para o cidadão em geral, dado o alarmismo que muitas vezes o tema suscita. A título de exemplo, é verdadeiramente arriscado assumir que a "cibersegurança preocupa mais de 90% das empresas portuguesas" (Murgeira, 2018) quando o trabalho que serve a esta assunção da comunicação social assenta numa amostra de 80 indivíduos (KPMG, 2018). Ainda que longe desta ordem de grandeza de "mais de 90%", é de facto possível encontrar em outros trabalhos e inquéritos focados no quadro português, ainda que em escassa quantidade, elevadas percentagens no que respeita à eventual preocupação com os riscos por parte das organizações (AP2SI, 2016; Cardoso, *et al*., 2017; MARSH, 2018).

Um dado que poderia também indiciar a existência de uma maior consciencialização por parte das organizações, especialmente em Portugal, para a necessidade de implementação de medidas de proteção dos seus sistemas de informação, seria considerarmos o significativo aumento do número de certificações na norma ISO/IEC 27001[60] registado em 2016. Em Portugal, as certificações aumentaram em 71,5%, enquanto a nível global esse aumento foi de 21%[61]. No entanto, investigadores e peritos, quando consultados e entrevistados no âmbito do nosso trabalho sobre o domínio da certificação e normalização, sugerem-nos que este crescimento não chega ainda ao que Portugal deveria ter em relação ao conjunto dos países Europeus e em relação ao número de organizações nacionais existentes. Sugerem-nos também que muito deste crescimento poderá resultar de exigências externas, isto é, da certificação como condição imposta por organizações estrangeiras com ligações e relações com o tecido empresarial português, pelo que seria extemporâneo assumir que tal crescimento terá origem num eventual aumento da preocupação com a segurança do risco digital. A ideia de esta exigência de mercado, tanto ao nível nacional como internacional, como fator impulsionador para a realização de certificações e normalização por parte das organizações, especialmente as do setor

[60] A família da norma ISO/IEC 27000 compreende a gestão de sistemas de segurança da informação. A norma ISO/IEC 27001 "especifica os requisitos para estabelecer, implementar, manter e melhorar de forma continuada um sistema de gestão da segurança da informação dentro do contexto da organização. Inclui também requisitos para a avaliação e tratamento de riscos de segurança da informação adaptados às necessidades da organização. Os requisitos estabelecidos na ISO/IEC 27001:2013 são genéricos e adaptáveis a todas as organizações, independentemente do tipo, tamanho ou natureza." Em https://www.iso.org/standard/54534.html consultado em 28 de maio de 2018.

[61] Das 12 532 certificações na norma ISO/IEC 27001 na Europa em 2016, Portugal tem apenas 96 (56 em 2015). Neste plano, Reino Unido (com 3 367 certificações), Alemanha (1 338 certificações), Itália (1 220 certificações), Espanha (752 certificações) e Holanda (670 certificações) são os países Europeus que integram a classificação dos 10 países com maior número de certificações à escala mundial. Dados recolhidos no "ISO Survey of Management System Standard Certifications 2016", disponível em https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 consultado em 28 de maio de 2018.

privado, determinando, assim, a implementação de mecanismos com vista à proteção das suas infraestruturas e dos seus sistemas de informação, é igualmente partilhada pelo GNS/CNCS[62].

Independentemente das causas, seja pelo alarme social, pelo mediatismo ou pela exigência externa, e esta pode resultar das relações entre organizações ou dos quadros normativos e legais em que operam, pelos dados disponíveis é possível assumir que, em Portugal, ainda que não em níveis que poderiam ser considerados desejáveis[63], existirá algum nível de conhecimento por parte das organizações, colaboradores e gestores, para os riscos de segurança digital e, por conseguinte, para a necessidade de políticas internas das organizações focadas nestes, contando com o envolvimento dos decisores de topo na sua planificação e implementação (AP2SI, 2016; Cardoso, *et al.*, 2017). No entanto, os dados disponíveis parecem sugerir que o aumento dos incidentes – intencionais e não intencionais – e dos crimes informáticos em Portugal e no estrangeiro, bem como o desta aparente maior consciencialização das organizações para os riscos de segurança digital, não são acompanhados uniformemente por uma prática financeira nas organizações, nomeadamente em termos de um aumento, que seria de esperar, nos seus orçamentos dedicados à implementação de instrumentos e mecanismos de gestão do risco. As causas desta constatação são impossíveis de retirar através dos estudos atualmente disponíveis. Da mesma maneira que alguns destes estudos agregam todo o tipo de organizações, sem que existam dados que permitam uma desagregação por dimensão ou tipo, e às vezes por setor, também a questão financeira em alguns trabalhos é suscetível de criar confusão por não distinguir despesa em TIC e despesa em gestão do risco.

Sabendo-se que a "cibersegurança tem custos" e que a "justificação de recursos dedicados à cibersegurança – que é percecionada sobretudo como ameaça hipotética – torna-se, portanto, mais complicada dada a disponibilidade limitada de dados concretos em como investimentos nesta área obtêm resultados concretos" (Pawlak e Wendling, 2013: 537), a maioria das organizações e indivíduos consultados em Portugal sobre esta matéria, e que sobre ela responderam, manifesta uma estabilização ou manutenção dos orçamentos disponíveis para estas atividades em relação a anos anteriores (AP2SI, 2016; Cardoso, *et al*., 2017; MARSH, 2018). Já a nível global, através dos resultados disponíveis em trabalhos internacionais, parece existir uma movimentação em sentido diferente. Não obstante o reconhecimento, a nível internacional, de que os constrangimentos com as questões orçamentais são o primeiro obstáculo ou desafio para a cibersegurança das organizações (BBB, 2017; EY, 2016), e onde cerca de 62% dos gestores de topo internacionais questionados admitem não ter a intenção de aumentar a despesa das suas organizações com cibersegurança perante uma quebra de segurança que não revele provocar danos aparentes (EY, 2016: 9) – o que poderá indiciar que se trata de uma situação que resulta de uma eventual avaliação em que o risco poderá ser aceitável para as organizações –, 86% dos inquiridos reconhece a necessidade de um aumento na ordem dos 50% do

[62] Em entrevista realizada em 11 de setembro de 2018.

[63] Assunção retirada do conjunto de entrevistas realizadas no âmbito deste trabalho. Todos os entrevistados, ainda que identificando progressos ao longo dos anos, manifestaram ter a perceção de existir ainda alguma falta de conhecimento e sensibilização nas organizações, em especial nas empresas, para os riscos resultantes da transformação digital, nomeadamente dos riscos de segurança digital, que importa colmatar.

seu orçamento para esta área (EY, 2016: 15). No entanto, os dados indicam também que pouco mais de metade dos gestores internacionais, 53% dos inquiridos, reconhece ter efetivamente aumentado os seus orçamentos nesta área durante os 12 meses anteriores ao questionário (EY, 2016: 15). São sensivelmente na mesma ordem de grandeza, 55% dos inquiridos, aqueles que manifestaram a intenção de aumentar os seus orçamentos nos 12 meses subsequentes ao questionário que tomamos como referência (EY, 2016: 15).

Como já aqui referimos, apesar dos múltiplos exercícios de tentativa de aferição de custos e perdas para a economia, e para as empresas, em resultado de incidentes decorrentes da utilização da informação nos ambientes digitais, existe um claro vazio de informação. Mas este vazio de informação também se encontra ao nível dos custos e investimentos com a implementação de mecanismos de proteção e gestão do risco de segurança digital, considerando ainda que a estes acrescem custos decorrentes da implementação, manutenção e utilização da infraestrutura digital das organizações. Ou seja, o custo da segurança nas organizações resulta duma agregação de custos diretos – com a implementação e manutenção da tecnologia – e indiretos – decorrentes da utilização destes mecanismos, e.g. "como o tempo perdido devido ao esquecimento de credenciais, a inconveniência na transferência de dados entre zonas de segurança ou incompatibilidades entre mecanismos de segurança que atrasam processos essenciais" (Böhme, 2010) e mesmo em resultado de decisões menos informadas na sequência de informação não disponível ao decisor pela sua retenção em processos de segurança e de privacidade (Böhme, 2010). Nestes há ainda que considerar a existência de custos fixos e custos variáveis. Dadas as especificidades técnicas e humanas que a cibersegurança implica para as organizações, dentro daquelas que são as orientações e boas práticas macro comummente aceites ou tidas como referência (OCDE, 2012a; 2015a; Paulsen e Toth, 2016a; FERMA, 2017), ou de normas e metodologias internacionalmente reconhecidas como as definidas pela ISO/IEC, NIST, OCTAVE, etc. (IDN-CESEDEN, 2013; Pereira e Santos, 2014), os modelos, mecanismos e, como consequência, os custos associados à sua implementação variam de organização para organização. Na perspetiva de investigadores e peritos entrevistados no âmbito deste trabalho, este deve ser visto como o principal erro em que as organizações, e em especial as empresas, incorrem, aumentando, assim, substancialmente os riscos para a sua atividade: abraçar a transformação tecnológica no ambiente organizacional, sejam quais forem os incentivos na origem dessa mudança, sem previamente se questionarem ou fazerem avaliações aprofundadas dos riscos decorrentes do facto dos dados e da informação passarem a estar disponíveis e a serem utilizadas num formato diferente do considerado tradicional, isto é, as ameaças não são devidamente avaliadas, privilegiando-se de imediato as anunciadas vantagens, e já aqui referidas, da transformação digital. Nesta linha de pensamento sobre as prioridades assumidas pelas organizações, encontramos também a COTEC Portugal: "Com a pressão para colocar rapidamente a inovação no mercado, os líderes empresariais e os responsáveis pela inovação não consideram a segurança como essencial. Não é prioritária e, em muitos casos é mesmo desconhecida" (Monteiro, 2018). Este perigo ganha um relevo ainda maior quando observado à luz das PME.

Dada a escassez de informação publicamente disponível, sendo que quando existem referências a custos elas fazem alusão a montantes globais ou a causas parciais[64], e pelas suas implicações, apenas poderemos deduzir que a implementação de mecanismos de gestão do risco de segurança digital se revela de algum peso financeiro e orçamental, especialmente para as PME, pelo que se considera que estas "não se podem permitir errar quando se comprometem com investimentos importantes e potencialmente dispendiosos, e necessitam de ser eficazes o tanto quanto possível na afetação de recursos" (BBB, 2017: 3). Esta proposição pode encontrar alguma base de sustentação no exercício anualmente conduzido pelo Governo do Reino Unido na elaboração do "Cyber Security Breaches Survey", onde, na secção dedicada ao investimento em cibersegurança, é possível observar que "a variação dos gastos é muito superior entre as grandes empresas […], com as maiores empresas a terem capacidade e possibilidade de optar por gastar quantias muito elevadas ou relativamente pequenas em cibersegurança" (Department for Culture Media & Sport, 2017: 21). Se a edição de 2018 deste questionário do Reino Unido confirma, naquele país, uma despesa média pelas médias empresas "significativamente mais elevada em termos reais (considerando a inflação) de £41.600, comparada com £15.500" indicados no questionário de 2017, parece também indicar um menor investimento nesta área pelas micro ou pequenas empresas – uma média de £2.200 de investimento em 2018 comparado com uma média de £2.600 investidos em 2017 (Department for Culture Media & Sport, 2018: 17). "Analisando os valores medianos de despesa, as micro ou pequenas empresas tendem a gastar um montante muito pequeno, pouco mais do que o custo de uma assinatura anual de software de antivírus ou antimalware, enquanto a típica grande empresa gasta num nível mais parecido com o de um salário anual de um indivíduo" (Department for Culture Media & Sport, 2017: 21).

Se, por um lado, nos poucos trabalhos disponíveis sobre o quadro português, uma aparente maior consciencialização para os riscos não parece ser acompanhada ao nível dum reforço financeiro ou orçamental nas organizações consultadas, por outro, em matéria de sensibilização e de formação para os riscos de segurança digital, são ainda em maior número aquelas que não desenvolvem ações

[64] A título de exemplo, o Better Business Bureau, uma organização que tem o foco da sua atividade na América do Norte (Canadá, EUA e México), usa a estimativa de uma despesa global em segurança da informação na ordem dos 170 mil milhões de dólares até 2020 (BBB, 2017: 3). Ainda, em Pawlak e Wendling, é referido o caso do estudo conduzido pelo Ponemon Institute e pela Bloomberg, em 2012, que concluiu que para "alcançar o nível de segurança de TI mais elevado possível (*i.e.* capacidade para repelir 95% dos ataques) significaria aproximadamente um aumento em nove vezes das despesas das empresas dos atuais 5,3 mil milhões de dólares (combinados) para 46,6 mil milhões de dólares" (2013: 538). Do mesmo Ponemon Institute, patrocinado pela empresa IBM, um estudo divulgado em julho de 2018 refere que, em 2017, com base em inquéritos a 477 organizações distribuídas por 15 países, foi possível concluir que, em média, o custo com a perda ou violação de dados, que inclui não só a perda direta mas também os custos associados com deteção, resposta e notificação de incidentes, foi de 3,6 milhões de dólares. Ainda se conclui que esse custo aumentou em 6,4% em relação ao ano anterior e que, em média, o custo por cada dado perdido pelas organizações foi de 148 dólares. No entanto, este estudo apresenta um âmbito limitado dado que se foca apenas na perda e violação de dados, deixando de fora custos com outro tipo de incidentes como são a negação de serviço, isto é, a inatividade ou inoperância das empresas em resultado de incidentes, ou danos de reputação, entre outros (Ponemon Institute, 2018).

junto dos colaboradores por forma a criar uma consciência para os riscos, para a sua ação e para a reação (AP2SI, 2016; Cardoso, *et al*., 2017). Os dados mostram ainda a responsabilidade da gestão das atividades focadas nos riscos de segurança digital das organizações concentrada nos seus departamentos e áreas de gestão das TIC (AP2SI, 2016; Cardoso, *et al*., 2017; KPMG, 2018; MARSH, 2018).

Independentemente do reconhecimento da escassez de recursos qualificados em matéria de cibersegurança, tanto a nível internacional como a nível nacional, pelas empresas, pela academia e pelos decisores públicos (EY, 2016; Center for Cyber Safety and Education e (ISC)^2, 2017; Comissão Europeia, 2017a; Nóbrega, 2017; Pequenino, 2018) e, uma vez mais, não dispondo de dados que permitam estabelecer uma relação direta, apenas poderemos partir da proposição de que as razões para a falta de ações de sensibilização e formação para os riscos de segurança digital nas organizações, assim como a concentração da responsabilidade de ação nesta matéria nos departamentos de TIC, porque é ali que se concentra o conhecimento e a eventual especialização necessária para lidar com estes novos ambientes digitais, resulta do menor envolvimento dos decisores de topo nas políticas de segurança das organizações (EY, 2016; Cardoso, *et al.*, 2017). Importa referir que esta proposição é reforçada pelos testemunhos recolhidos junto de investigadores e peritos entrevistados que, decorrente da sua experiência e atividade – seja de investigação, docência e relação com as organizações, onde se incluem as empresas –, encontram no desconhecimento e impreparação dos decisores para estas matérias as principais razões. Nesta matéria, na entrevista feita no âmbito deste trabalho, a AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação, deixa muito claro qual, no seu entendimento, será "um dos maiores entraves aos temas da segurança" e à "gestão da mudança interna" das organizações: "enquanto os quadros decisores entenderem que a segurança/gestão do risco são temas que pertencem à informática e não a eles próprios, não iremos assistir a uma evolução positiva do tema"[65].

Parece existir, assim, e a partir destes testemunhos, uma perceção da falta de preparação dos gestores para compreenderem a necessidade de funcionamento integrado das diversas áreas das organizações no que toca às questões de cibersegurança, neste caso, das empresas. Podendo encontrar-se no Inquérito Aberto à Segurança da Informação nas Instituições em Portugal, conduzido pela AP2SI, uma eventual refutação desta proposição com a indicação de que "73,3% dos colaboradores reportaram que [a política de segurança da informação na instituição] foi emitida pela gestão de topo, assim como 83,8% dos diretores" (AP2SI, 2016: 6), é preciso contextualizar que estas percentagens se encaixam no universo de organizações que manifestaram dispor ou conhecer a existência destas políticas internas, ou seja "55,2% dos colaboradores indicaram a sua existência, assim como 75,5% dos diretores" (AP2SI, 2016: 6). Além do mais, a ideia de uma política de segurança da informação "emitida pela gestão de topo" não nos pode conduzir à assunção de que tal signifique existir o necessário envolvimento ativo desses gestores na sua definição e implementação.

[65] Resposta da AP2SI à entrevista escrita.

Segundo as orientações da ENISA nesta matéria, podemos observar que estas são situações que estão longe de constituir um contributo para a definição e implementação de uma cultura de cibersegurança nas organizações:

> alterações aos ambientes de trabalho nas organizações requerem responsabilidades claras e o envolvimento de todos dentro da organização, incluindo a gestão superior, promovendo uma apropriação do programa [de cultura de cibersegurança] e a motivação para a ele aderir. O compromisso com a cibersegurança deve ser assinalado através da disponibilização orçamental suficiente e a motivação para uma maior segurança em vez da simples conformidade de requisitos (ENISA, 2017a: 15).

Sendo que a existência, ou não, de uma cultura de cibersegurança nas organizações, incluindo empresas, tem uma enorme dependência da forma como as questões sobre segurança da informação assumem um papel no funcionamento, nos hábitos e na conduta diária das pessoas que as integram, assume-se com facilidade que o não envolvimento de todas as áreas internas das organizações na sua definição e implementação compromete seriamente a sua cibersegurança o que, consequentemente, poderá também comprometer seriamente a sua própria atividade.

A conjugação destas duas variáveis, isto é, um aparente menor envolvimento de todas as áreas internas das organizações[66] na definição, implementação e desenvolvimento de políticas internas dirigidas ao risco de segurança digital e a transferência para os departamentos ou áreas TIC de grande parte da responsabilidade em lidar com a informação das organizações nos ambientes digitais, poderá permitir inferir que as organizações apostam em grande medida por processos de transformação digital assentes em estratégias de informatização com pouca ou inexistente correlação com as restantes áreas funcionais (Hess, *et al.*, 2016). Mas, independentemente das estratégias de transformação digital adotadas pelas organizações, a definição e o impulso para a implementação de políticas centradas na gestão do risco de segurança digital nas organizações depende bastante, como já abordámos, de duas áreas nevrálgicas: os decisores, de topo e intermédios, e os profissionais com competências em TIC.

No entanto, a especial atenção nas pessoas que constituem estas duas áreas, não deve desviar a atenção do papel essencial que as restantes pessoas desempenham na aplicação de uma cultura de cibersegurança nas organizações. Olhando para a parte específica das organizações que propusemos como principal foco do nosso estudo, as empresas, e em particular as PME, cuja primeira razão de existência é a legítima persecução do lucro, os papéis que estas duas áreas nevrálgicas assumem são proporcionais à dimensão da própria empresa. Se numa grande empresa um conselho de administração poderá dispor, internamente, de assessoria e apoio à decisão que lhe permita avaliar as condições necessárias para o investimento na área da cibersegurança, incluindo a contratação de recursos humanos qualificados para o desenvolvimento e implementação desta área, as empresas de menor dimensão estarão mais limitadas nesse aspeto, a todos os níveis. Em determinados casos, nas

[66] Neste campo os trabalhos que estamos a usar como referência são dissonantes. Em Cardoso, *et al.*, (2017) parece existir um menor envolvimento dos gestores na definição e gestão das políticas de gestão do risco digital, quando existem, e em AP2SI (2016) este envolvimento foi declarado, tanto por gestores como por colaboradores, como sendo significativamente maior.

PME, a área dos sistemas de informação é mais uma entre as várias áreas organizacionais sob a responsabilidade de um dos quadros da empresa, quando não sujeita a subcontratação, sendo que nos casos das micro empresas essa é, muitas vezes, uma responsabilidade direta do empresário.

III.3. As qualificações

É neste quadro, e num momento que se verifica que "o digital é cada vez mais o modo de vida das empresas" (Sousa, 2018), que importa não só dispor de meios de aquisição de competências transversais adequada aos gestores e quadros superiores – seja nas grandes empresas ou PME – como a profissionais na área das TIC. Num exercício de consulta à oferta educativa em Portugal, em 2018, identificámos 12 cursos superiores dedicados à área da cibersegurança e que sintetizamos no quadro 3.2).

Quadro 3.2 – Oferta educativa superior específica para a área da cibersegurança em Portugal, em 2018.

Curso técnico superior profissional (4)	**Licenciatura – 1.º ciclo (1)**	**Mestrado – 2.º ciclo (6)**	**Doutoramento – 3.º ciclo (1)**
Cibersegurança (2)	Segurança Informática em Redes de Computadores (1)	Segurança Informática (3)	Segurança de Informação (1)
Redes e Segurança Informática (1)		Segurança de Informação e Direito no Ciberespaço (1)	
Cibersegurança, Redes e Sistemas Informáticos (1)		Engenharia de Segurança Informática (1)	
		Cibersegurança e Informática Forense (1)	

Legenda: quadro dos cursos identificados na área da cibersegurança ministrados em Universidades e Politécnicos em Portugal (fonte: Direção-Geral do Ensino Superior, http://www.dges.gov.pt/pt/pesquisa_cursos_instituicoes, consultado em 13 de junho de 2018)

A primeira constatação que retiramos deste quadro, que exclui a oferta disponível ao nível de "pós-graduação"[67], é a de que a maioria da oferta educativa superior em matérias especificamente relacionadas com a cibersegurança é disponibilizada ao nível dos 2.º e 3.º ciclos, isto é, em mestrados e doutoramentos, com exceção para uma licenciatura e quatro cursos técnicos superiores profissionais. Admitindo que a oferta educativa superior noutras áreas das TIC, como Engenharia Informática, Informática e Gestão de Empresas, Engenharia de Telecomunicações e Informática, Gestão de Sistemas de Informação ou Informática e Gestão[68], possam existir algumas abordagens à dimensão organizacional das empresas e das organizações, ainda que incipientes, uma rápida análise aos planos de estudos dos cursos apresentados neste quadro revela uma enorme incidência nas vertentes técnicas das TIC e, num grau substancialmente inferior, algumas unidades curriculares relacionadas com ética, legislação e análise de risco. Devemos salientar aqui uma exceção verificada num curso de mestrado sobre Segurança de Informação e Direito no Ciberespaço, dado o seu foco ter uma predominância no Direito e ter, ainda, componentes dedicadas à segurança nas organizações. Não se identificam, nestes planos de estudos, uma relação explícita com as vertentes de gestão empresarial ou organizacional encontradas em cursos relacionados com organizações e/ou empresas[69].

Investigadores e peritos por nós entrevistados, que reconhecem a superior capacidade técnica em TIC dos alunos formados nas instituições de ensino superior em Portugal, quando questionados sobre se a formação superior nessa área, e em especial a que se relaciona com a cibersegurança, contempla ou permite margem para uma abordagem multidisciplinar, seja na vertente organizacional como na vertente social, reconhecem que apesar de individualmente os docentes da área das TIC terem a perceção dessa necessidade, tal não sucede devido a uma "cristalização"[70] do sistema e das formas de ensino que não permitem, atualmente, acomodar o modelo multidisciplinar na oferta educativa. Entre estes investigadores e peritos há mesmo quem refira que apesar da importância e do contributo que estes cursos – em particular as licenciaturas apresentadas no quadro – representam para o desenvolvimento de competências na área da segurança da informação e da engenharia informática, deve questionar-se ou tentar perceber-se se a cibersegurança, por não dispor de metodologias próprias e porque deve ser relacionada transversalmente com outras áreas, das

[67] Com a ressalva de que a lista de cursos anunciados no sítio da Internet da ENISA é de preenchimento voluntário e que a responsabilidade de atualização da informação recai sobre quem procede ao seu registo, para uma ideia da oferta educativa ao nível de pós-graduações disponível em Portugal cf. https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities consultado em 1 de janeiro 2018.

[68] Tomámos como referência os cursos ao nível de licenciatura e mestrado do ISCTE - Instituto Universitário de Lisboa.

[69] Admitimos que estas relações possam eventualmente existir em pós-graduações que não analisamos no contexto deste trabalho.

[70] Expressão utilizada por um investigador numa entrevista realizada em 30 de maio de 2018.

organizações e da própria sociedade, se configura como disciplina autónoma, pelo que, nesta linha, deveria ser encarada mais como "um objeto de estudo, não uma disciplina"[71].

III.4. Representação e sinergias entre organizações

No momento em que a transformação digital parece ser um processo em curso impossível de travar e até mesmo de desacelerar, uma questão para a qual parece ser impossível, neste momento, encontrar uma resposta conclusiva, é a do porquê não existir uma maior preocupação com as questões da segurança no momento da transformação digital. A falta de sensibilização para a exposição aos riscos, a falta de preparação e de conhecimento por parte dos gestores e dos empresários para uma avaliação dos riscos nas organizações, a ausência de competências para reconhecer a necessidade de um investimento ao nível da cibersegurança ou os custos de implementação de mecanismos de avaliação, deteção e mitigação dos riscos – potenciais razões apontadas pelas entidades por nós entrevistadas e por alguma da bibliografia consultada no âmbito deste estudo – poderão representar hipóteses para o problema que representa a adoção da transformação digital onde apenas os benefícios, por vezes imediatos, para as organizações são os únicos fatores tidos em conta na ponderação.

Num quadro como o que aqui já abordámos em que, segundo os dados disponibilizados pelo COMPETE 2020, em termos de projetos aprovados, cerca de 80% são captados pelas PME, foi-nos referido que, sem dados disponíveis que possam aferir o grau de preocupação nesta matéria, no universo de candidaturas muito abrangente no sistema de incentivos, uma parte significativa destas não apresentam uma "preocupação muito disseminada"[72] com os aspetos dos riscos de segurança digital. No entanto, um dado que certamente poderá contribuir para uma futura resposta é o facto de, ao nível dos incentivos, sejam eles dedicados a projetos inovadores ou a novos modelos de negócio, relacionados com a política definida em Portugal em matéria de "Indústria 4.0", existirem instrumentos de incentivos e financiamento – através da elegibilidade de despesas – que cobrem também aspetos relacionados com as questões de cibersegurança, incluindo, por exemplo, apoios para diagnósticos de situação e definição de estratégias enquadrando políticas internas de segurança, para certificações, equipamentos e até contratação de recursos humanos[73].

Para além das organizações com uma missão pública junto do tecido empresarial português, destacando-se entre elas obrigatoriamente o IAPMEI[74], em Portugal existe um alargado leque de

[71] Citação retirada de uma entrevista realizada em 14 de junho de 2018.

[72] Citação retirada da entrevista a um gestor público realizada em 15 de junho de 2018.

[73] Cf. IAPMEI, 2017. Para além desta documentação disponibilizada pelo IAPMEI, algumas destes esclarecimentos resultaram de entrevistas realizadas, nomeadamente com um gestor público e especialista em incentivos.

[74] Cuja missão é a de "promover a competitividade e o crescimento empresarial, assegurar o apoio à conceção, execução e avaliação de políticas dirigidas à atividade industrial, visando o reforço da inovação, do empreendedorismo e do investimento empresarial nas empresas que exerçam a sua atividade nas áreas sob

grupos de interesse legítimos[75] enquadrados no que Bobbio *et al.*, definem como "associacionismo voluntário" e "associações patronais" (2004: 64-68). Estas organizações de índole privada não só aparentam dispor de um maior poder de representação, nacional e internacional, com vista a "influenciar os poderes públicos num sentido favorável aos interesses a seu cargo" (Chagnollaud, 1999: 100) como se apresentam junto dos seus associados com uma missão que se diz de promoção e apoio ao desenvolvimento das empresas. Algumas delas oferecendo mesmo serviços de consultoria ou de formação o que, na perspetiva das PME, pode representar um meio de colmatar algumas deficiências de nível funcional das empresas, seja pelo peso financeiro que determinadas ações representam para as empresas, seja pelo nível de competências, muitas vezes avançadas, que requerem para a sua implementação. Espera-se, por isso, que estas organizações representem, teoricamente, a agregação dos interesses e prioridades definidas pelos seus associados. Em Portugal, pelo seu mediatismo e pela aparente maior representação do tecido empresarial, consideram-se relevantes as seguintes organizações[76]:

- AEP - Associação Empresarial de Portugal, Câmara de Comércio e Indústria que, na sua página de Internet, não dispõe de informação pública sobre a sua representatividade[77];
- AIP-CCI – Associação Industrial Portuguesa – Câmara de Comércio e Indústria que, segundo a sua página de Internet, tem 55.102 associados diretos e indiretos cujo volume de negócios dos associados diretos é de 20,3 mil milhões de euros[78];
- CCP – Confederação do Comércio e Serviços Portugal que, na sua página de Internet, não dispõe de informação pública sobre a sua representatividade[79];

---

tutela do Ministério da Economia, designadamente das empresas de pequena e média dimensão, com exceção do setor do turismo e das competências de acompanhamento neste âmbito atribuídas à Direção-Geral das Atividades Económicas." (fonte: https://www.iapmei.pt/SOBRE-O-IAPMEI/Missao-Visao-Valores.aspx consultado em 20 de junho de 2018).

[75] Sobre grupos de interesses ver Chagnollaud, 1999: 100-103; Carvalho, 2000; Gibson, 2000; Lampreia e Guéguen, 2008.

[76] No âmbito deste trabalho, foram solicitadas entrevistas a todas as Associações e Confederações aqui indicadas, especificando o seu objetivo e o enquadramento das preocupações em torno da cibersegurança e das empresas. Apesar das insistências, apenas foram obtidas reações da CCP, que não forneceu respostas mesmo tendo manifestado a sua disponibilidade para participar neste exercício, e da CIP, que indicou não se encontrar habilitada com respostas que pudessem ir ao encontro do objetivo deste trabalho.

[77] Que desenvolve "um conjunto de ações, designadamente prestação de serviços à comunidade empresarial nos domínios das feiras, exposições, congressos, informação e apoio às empresas, consultoria, formação profissional, missões empresariais, promoção de negócios e investimentos, […]" (fonte: http://www.aeportugal.pt/ ("Apresentação") consultado em 20 de junho de 2018).

[78] Que tem entre os seus objetivos "promover o desenvolvimento sustentado das atividades económicas portuguesas e, em especial, contribuir para o progresso das empresas e das associações suas filiadas, nos domínios, económico, organizativo, comercial, técnico, tecnológico, associativo, cultural e social, dando sempre prioridade ao apoio às Pequenas e Médias Empresas" (fonte: alínea *b)* do Artigo 3.º dos Estatutos em http://www.aip.pt//uploads/AIP/Estatutos_AIP-CCI_31-03-2015.pdf consultado em 20 de junho de 2018).

- CIP – Confederação da Indústria Portuguesa que, segundo a sua página de Internet, representa "114.566 empresas, que empregam 1.541.539 trabalhadores e têm um volume de negócios de € 105.208 milhões"[80];
- COTEC Portugal - Associação empresarial para a Inovação que, segundo a sua página de Internet, "engloba empresas multinacionais, grandes grupos nacionais e PME's, em vários setores de atividade, representando, em termos agregados, mais de 16% do PIB em valor acrescentado bruto e 8% do emprego privado"[81].

Numa tentativa de identificarmos o foco destas organizações em matéria de cibersegurança, e sem possibilidade de recolher informação através de fontes primárias[82], optámos pelo exercício de pesquisa nas suas páginas de Internet, por forma a obter informação publicamente disponível. Neste exercício apenas obtivemos resultados diretos sobre "cibersegurança" nas páginas da CIP e da COTEC[83]. Sem que isso se possa constituir como um indicador inequívoco das atividades desenvolvidas pelas organizações em prol dos seus associados nesta área, podendo apenas ser o resultado das suas estratégias comunicacionais com o público, pode deduzir-se um maior efeito de comunicação da preocupação com as questões de cibersegurança pela CIP e, com uma ainda maior relevância, pela COTEC (ver Anexo E). No entanto, importa referir que, segundo a informação que nos foi prestada pela CIP[84], a cibersegurança será uma das áreas da agenda do recentemente criado órgão consultivo desta Confederação, o Conselho Estratégico para a Economia Digital[85], no âmbito da temática da transformação digital. Destaca-se também na COTEC o lançamento por parte desta

[79] Que tem como uma das suas atribuições "organizar e desenvolver serviços destinados a apoiar os associados, nomeadamente através da elaboração de estudos e apoio de consultadoria, visando reforçar a capacidade de atuação das empresas do setor" (fonte: http://www.ccp.pt/CCP/pt-PT/33/-1/Content.aspx consultado em 20 de junho de 2018).

[80] Com a missão de "contribuir para o progresso da economia de mercado e da iniciativa privada" e "apoiar as empresas de todas as dimensões e setores", entre outras (fonte: http://cip.org.pt/quem-somos/apresentacao/ consultado em 20 de junho de 2018).

[81] Que visa "a promoção da inovação e cooperação tecnológica empresarial" (fonte: http://www.cotecportugal.pt/pt/quem-somos/cotec-portugal-associacao-empresarial-para-a-inovacao consultado em 20 de junho de 2018).

[82] Pelas razões expostas anteriormente sobre a realização de entrevistas, as únicas fontes de informação a que pudemos recorrer para identificar eventuais iniciativas e ações desenvolvidas por estas organizações sobre cibersegurança restringiram-se a fontes disponíveis na Internet e na comunicação social.

[83] Este exercício de pesquisa foi realizado, em todas as páginas, no dia 12 de abril de 2018 e repetido no dia 25 de maio de 2018. Em 12 de abril de 2018 apenas obtivemos resultados na página da COTEC. Em 25 de maio de 2018 foi possível obter resultados na página da COTEC e também da CIP.

[84] Em resposta escrita, em 10 de setembro de 2018, ao nosso pedido de entrevista de 4 de junho de 2018.

[85] A composição deste órgão consultivo permite identificar entidades que se têm destacado pela sua atividade em matérias de cibersegurança e privacidade. Cf http://cip.org.pt/economia-digital-debatida-na-cip/ consultado em 10 de setembro de 2018.

associação empresarial de uma "área de atividade dedicada à reflexão sobre cibersegurança, à promoção de ferramentas de resiliência, à partilha de boas práticas e ao estabelecimento de redes de colaboração entre organizações públicas e privadas com vista ao estímulo da boa governança nesta área"[86]. Longe de podermos retirar desta observação uma conclusão sobre uma maior ou menor atenção por parte das empresas, e também das organizações que as representam, apenas podemos constatar que os dados disponíveis e possíveis de observar parecem indicar, de certa forma, um alinhamento com as preocupações que anteriormente expusemos e identificámos sobre a atenção e a prioridade atribuída pelas empresas e decisores – empresários e gestores – à cibersegurança nas suas organizações.

III.5. As políticas públicas

Como já aqui referimos, o impacto, económico e social, nas empresas e nos Estados, que decorre de incidentes – intencionais e não intencionais – ao nível do digital pode ser significativo, ainda que não mensurável pelas razões a que também já aludimos. Por razão dessa crescente perceção do risco por parte dos decisores públicos, as Organizações Internacionais e os Governos são levados a definirem estratégias em "que a segurança do ciberespaço seja considerada como uma prioridade nacional" (Presidência do Conselho de Ministros, 2015). Nesse sentido, o Governo português não foi exceção e adotou, em junho de 2015, a Estratégia Nacional de Segurança do Ciberespaço (ENSC)[87]. Enveredando por uma comparação com outros países, e tomando como referência temporal estratégias europeias especificamente dirigidas para a cibersegurança e o ciberespaço como as implementadas pela Estónia em 2008 (Osula, 2015a), Eslováquia em 2009 (Hriciková e Kaska, 2015), Reino Unido em 2009 (Osula, 2015), Lituânia em 2011 (Butrimas, 2015), França em 2011 (Brangetto, 2015), Países Baixos em 2011 (Kaska, 2015), Espanha em 2013 (Cendoya, 2016), Hungria em 2013 (Kovács e Szentgáli, 2015) ou Itália em 2013 (Glorioso, 2015), todas elas anteriores ou do ano da adoção da "Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido" na UE (Comissão Europeia, 2013), uma das questões que poderá surgir de imediato, e que fica sem resposta, é sobre as razões para que Portugal tenha adotado só em 2015, muitos anos após o advento da internet e da perceção dos riscos inerentes à sua utilização, uma estratégia com este foco[88].

Dos cinco pilares que sustentam esta ENSC, todos eles com relevância para o tema que aqui discutimos, destacamos os pilares da subsidiariedade, da complementaridade e da proporcionalidade[89].

---

[86] Fonte http://www.cotecportugal.pt/pt/oquefazemos/think-tank/ciberseguranca/ciberseguranca20170822110846/ consultado em 25 de maio de 2018.

[87] Porque o nosso foco se prende na adoção inédita de uma estratégia especificamente para esta matéria em Portugal, escusamo-nos aqui, propositadamente, de fazer uma dissertação sobre todo o conjunto de legislação anterior, e o seu histórico, em matéria de segurança nacional onde as questões relacionadas com a segurança na Internet, das empresas, dos cidadãos e do Estado são, ainda que superficialmente, abordadas. Ver Anexo F.

[88] Importa destacar que para alguns destes países, tal como para Portugal, é possível encontrar legislação anterior com foco parcial e isolado em algumas das áreas que respeitam à segurança do ciberespaço.

[89] Os outros dois pilares são "cooperação" e "sensibilização".

Se o pilar da subsidiariedade designa uma hierarquia de responsabilidades na segurança do ciberespaço, dado que esta se inicia "no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais", este atribui ao setor privado a "responsabilidade primária pela sua proteção" dado que é este quem detém "grande parte das infraestruturas tecnológicas que compõem o ciberespaço" (Presidência do Conselho de Ministros, 2015). Uma vez que a "segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais" (Presidência do Conselho de Ministros, 2015), conforme define o pilar da complementaridade, não é muito claro em que medida assenta o pilar da proporcionalidade uma vez que, sem qualquer orientação, direta ou indireta, determina que os "riscos inerentes ao ciberespaço devem ser avaliados e geridos de forma adequada, assegurando-se a proporcionalidade dos meios e medidas para o seu exercício" (Presidência do Conselho de Ministros, 2015).

A ENSC estabelece quatro objetivos estratégicos, a saber, *a)* promover uma utilização consciente, livre, segura e eficiente do ciberespaço; *b)* proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; *c)* fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e *d)* afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação. Esta estratégia traduz-se "em seis eixos de intervenção, enformados em medidas concretas e respetivas linhas de ação, destinadas a reforçar o potencial estratégico nacional no ciberespaço" (Presidência do Conselho de Ministros, 2015):

Eixo 1 — Estrutura de segurança do ciberespaço;

Eixo 2 — Combate ao cibercrime;

Eixo 3 — Proteção do ciberespaço e das infraestruturas;

Eixo 4 — Educação, sensibilização e prevenção;

Eixo 5 — Investigação e desenvolvimento;

Eixo 6 — Cooperação.

Face a todo o enquadramento da transformação digital e da cibersegurança que aqui traçámos, o nosso entendimento é de que esta estratégia, que reconhece a "rápida evolução intrínseca ao ciberespaço e, consequentemente, a crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização" (Presidência do Conselho de Ministros, 2015), apresenta algumas fragilidades que escapam à lógica da segurança do ciberespaço como prioridade nacional. Tendo sido adotada em junho de 2015 sem apresentar aquilo que em Barbas e Sancho, é definido como "aproximação conceptual" (2018: 56), isto é, sem que defina conceptualmente o ambiente que pretende tornar seguro – o ciberespaço – ou o conjunto de recursos, processos e estruturas utilizados para o proteger e proceder à gestão do risco – a cibersegurança –, foi estabelecido um "prazo máximo de três anos" para a sua revisão, assim como a "verificação anual dos objetivos estratégicos e das linhas de ação e

adequação dos mesmos à evolução das circunstâncias" (Presidência do Conselho de Ministros, 2015). Sem "indicar prioridades nem metas palpáveis a alcançar" (Gouveia e Morgado, 2017: 8), à data de agosto de 2018 e ultrapassado esse prazo máximo, não são publicamente conhecidos quaisquer planos de ação para a sua implementação ou os resultados da sua avaliação[90]. Segundo o Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança (GNS/CNCS), a inexistência desse plano de ação e a realização de um "ponto de situação" tardio em relação ao que ficou definido na ENSC encontra razão de ser na ausência de definição e de criação de uma "estrutura de governação" da própria estratégia[91]. Acompanhamos também a discussão feita em Gouveia e Morgado, porque ela reforça a importância de uma clara definição quanto à implementação de estratégias, e esta não será exceção, sobre o facto de a ENSC referir "de forma abstrata a necessidade de estimular e apoiar iniciativas de investigação e desenvolvimento nos assuntos de segurança do ciberespaço" (2017: 8).

Sem uma definição conceptual, mas fazendo uma distinção do âmbito da cibersegurança e da ciberdefesa no seu "Eixo 1 – Estrutura de segurança do ciberespaço" e o do cibercrime no "Eixo 2 – Combate ao cibercrime", poder-se-á argumentar que uma estratégia que pretende "afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação" (Presidência do Conselho de Ministros, 2015) ficará aquém desse objetivo considerando não só os pontos referidos anteriormente mas também o foco praticamente exclusivo em medidas com vista à proteção de infraestruturas críticas nacionais. No que respeita às empresas, que se espera que também utilizem o ciberespaço de forma "livre, segura e eficiente", e a quem se atribui responsabilidades na segurança do ciberespaço como vimos antes, também se manifesta uma intenção de ver implementadas medidas, mesmo sem que se clarifique a forma e os instrumentos a utilizar. Neste campo, no âmbito do "Eixo 4 – Educação, sensibilização e prevenção", perspetiva-se a adoção de medidas que visem "promover campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas" e "estabelecer programas específicos para as Pequenas e Médias Empresas (PME), para as associações socioprofissionais e, em particular, para os profissionais liberais" (Presidência do Conselho de Ministros, 2015). No âmbito do "Eixo 5 – Investigação e desenvolvimento", são pretendidas medidas para "apoiar a participação da academia e das empresas nacionais em projetos de investigação e desenvolvimento internacionais" (Presidência do Conselho de Ministros, 2015). Se relativamente às entidades públicas e às infraestruturas críticas é ao Centro Nacional de Cibersegurança (CNCS) que cabe o papel de "coordenação operacional e de autoridade nacional em matéria de cibersegurança" (Presidência do Conselho de Ministros, 2015), em nenhuma destas medidas relacionadas com outros setores, e na ausência de um plano de ação, são designados os intervenientes ou os responsáveis pela sua definição e implementação – é, portanto, esperado que as ações e medidas necessárias à sua execução

[90] Sobre a avaliação da ENSC foi referido por Pedro Veiga, Coordenador demissionário do Centro Nacional de Cibersegurança, em audição na Assembleia da República na CACDLG, em 4 de julho de 2018, que "ainda não foi terminada a avaliação, a avaliação está a decorrer." (fonte: http://www.canal.parlamento.pt/?cid=3068&title=audicao-de-pedro-veiga-coordenador-demissionario-do-centro-nacional-d – declarações proferidas entre a 1h11m51s e 1h11m56s).

[91] Em entrevista realizada em 11 de setembro de 2018. As citações utilizadas nesta frase resultam de declarações proferidas pelo entrevistado.

decorram na e pela esfera setorial que as tutela. Esta foi uma situação que, como foi referido durante a entrevista ao GNS/CNCS[92], pelo facto de não existir de uma estrutura de governação definida na ENCS, constituiu alguma dificuldade, em 2016, na tentativa de alcançar áreas setoriais fora da sua esfera de competências no momento da realização do primeiro ponto de situação.

O foco nas infraestruturas críticas não só é visível ao longo da redação da própria ENSC como é reconhecido pelo Governo na Resolução do Conselho de Ministros n.º 115/2017 que constitui o grupo de projeto denominado Conselho Superior de Segurança do Ciberespaço (CSSC)[93]: "Visou-se [com a aprovação da ENSC], em especial, garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (Presidência do Conselho de Ministros, 2017). Com um conjunto de objetivos determinados para a ENSC, o CSSC, cuja criação, segundo o GNS/CNCS[94], pretendeu responder às dificuldades provocadas pela ausência de uma estrutura de governação, "tem por missão assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da respetiva revisão" (Presidência do Conselho de Ministros, 2017).

Quando a ENSC reparte a responsabilidade pela segurança do ciberespaço por diversos atores e reclama sinergias e cooperação, deve questionar-se o alcance e eficácia deste CSSC pelo facto de ser composto quase exclusivamente por entidades da Administração Pública – direta e indireta. Ressalvamos aqui o nosso "quase exclusivamente" dado que o "representante da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT)", ainda que não nessa qualidade, poderá ser proveniente do setor privado, uma vez que esta rede compreende entidades públicas e privadas[95]. Ainda, porque a convite do presidente deste CSSC poderiam "participar nos trabalhos do CSSC representantes indicados por outras entidades, bem como personalidades de reconhecido mérito na área em que são desenvolvidos os trabalhos" (Presidência do Conselho de Ministros, 2017). Neste CSSC inicialmente previsto, nota-se igualmente a ausência de representantes das Regiões Autónomas portuguesas – públicos e/ou privados – na sua composição.

Refira-se ainda que, com o objetivo de fazer a transposição da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JOUE, 2016a), foi admitida na Assembleia da República, em 26 de março de 2018, a Proposta de Lei n.º 119/XIII,

[92] Em 11 de setembro de 2018.

[93] A constituição do CSSC vigorou a partir de 25 de agosto de 2017 e estabelecia 30 dias como o prazo máximo para a aprovação de um regulamento de funcionamento interno. Esse regulamento foi aprovado mais de 90 dias depois, em 29 de novembro, e publicado em Diário da República apenas a 2 de fevereiro de 2018 (Presidência do Conselho de Ministros, 2018). Esta Resolução do Conselho Ministros foi revogada pela Lei n.º 46/2018, de 13 de agosto (Assembleia da República, 2018).

[94] Em 11 de setembro de 2018.

[95] Cf. http://www.redecsirt.pt/#membros

entretanto promulgada como Lei n.º 46/2018, de 13 de agosto[96], que prevê, com essa transposição, o estabelecimento do regime jurídico da segurança do Ciberespaço (Presidência do Conselho de Ministros, 2018a). Entre os diversos aspetos que a Lei n.º 46/2018 prevê implementar, consagra também o "Conselho Superior de Segurança do Ciberespaço, o Centro Nacional de Cibersegurança como a Autoridade Nacional de Cibersegurança, bem como o "CERT.PT" como a equipa de resposta a incidentes de segurança informática nacional" e ainda prevê quais "os operadores de serviços essenciais e os prestadores de serviços digitais" abrangidos pelo documento legislativo (Presidência do Conselho de Ministros, 2018a: 2). Sem entrarmos na apreciação desta Lei, pois alguns dos principais aspetos positivos e, principalmente, os negativos encontram eco nos pareceres emitidos por diversas entidades no âmbito do processo legislativo[97], o seu Anexo, que ao identificar setores e subsetores de operadores de serviços essenciais, parece excluir, claramente, grande parte do tecido económico português do âmbito desta legislação e do conjunto de incentivos, não financeiros mas coercivos, que define[98]. Sobre esta exclusão, não podemos deixar de destacar as dúvidas pertinentes inicialmente apontadas pela Comissão Nacional de Proteção de Dados (CNPD) sobre o âmbito de aplicação:

> Quanto ao âmbito da proposta de lei, suscitam-se dúvidas sobre o alcance da alínea *e)* do n.º 1 do artigo 2.º, quando se estabelece que a lei se aplica *a quaisquer outras entidades que utilizem as redes e sistemas de informação*, além de se aplicar à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais. Todas as obrigações estão definidas em função destes últimos atores. Apenas o artigo 20.º, sobre notificações voluntárias de incidentes, poderá abarcar outras entidades além das especificamente identificadas[99] (CNPD, 2018: 2v).

[96] Durante o período da redação deste trabalho, iniciou-se e concluiu-se o processo parlamentar, tendo a Proposta de Lei, depois de admitida na AR, baixado à comissão de especialidade, a CACDLG, em 15 de junho de 2018, e votada e aprovada com alterações, na especialidade em 11 de julho de 2018. Foi finalmente aprovada em votação final global em 18 de julho de 2018, quando a Diretiva da UE previa 9 de maio de 2018 como data limite para a adoção e publicação das "disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento" à Diretiva nos Estados-Membros (JOUE, 2016a: L194/25). O diploma foi apreciado e promulgado pelo Presidente da República em 2 de agosto de 2018 sob a designação de "Decreto da Assembleia da República nº 238/XIII […]" (http://www.presidencia.pt/?idc=10&idi=151712 consultado em 3 de agosto de 2018) e publicado como Lei n.º 46/2018, de 13 de agosto (Assembleia da República, 2018b).

[97] Cf. pareceres da CNPD, GNS, Comissão de Acesso aos Documentos Administrativos, Governo da RAA, Assembleia Legislativa da RAA, Governo da RAM, Assembleia Legislativa da RAM, do parecer e nota técnica da CACDLG, e da tomada de posição da APDSI em http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42367 consultado em 1 de julho de 2018.

[98] Para além dos operadores de serviços essenciais, também no que respeita aos prestadores de serviços digitais e aos requisitos de segurança definidos no Artigo 18.º parecem não subsistir dúvidas: "O presente artigo não se aplica às microempresas nem às pequenas empresas, tal como definidas pelo Decreto-Lei n.º 372/2007, de 6 de junho, na sua redação atual." (Presidência do Conselho de Ministros, 2018a)

[99] Itálicos no original.

Um outro aspeto que não podemos deixar de assinalar, tratando-se de uma situação inicialmente apresentada do diploma ainda na forma de Proposta de Lei, também ela referida no parecer emitido pela CNPD, e que nos parece conceptualmente grave: a atribuição à equipa de resposta a incidentes de segurança informática nacional da competência de "monitorizar o ciberespaço". Atendendo ao conceito de ciberespaço que aqui demos eco e, consequentemente, os recursos necessários que implicaria a sua execução tal como descrita, esta competência revelar-se-ia impossível de concretizar. Esta incoerência foi ultrapassada pelas alterações introduzidas durante o processo de apreciação parlamentar, passando, no documento final, a estar na esfera de competências desta equipa "monitorizar os incidentes com implicações a nível nacional" (Presidência do Conselho de Ministros, 2018b).

Ainda na vertente pública, julgamos importante destacar também o Programa de Segurança Económica (PSE) no âmbito do Serviço de Informações de Segurança (SIS) com características de sensibilização onde "as organizações portuguesas são desafiadas a refletir sobre a importância de proteger o conhecimento e a informação sensível, num mundo concorrencial e simultaneamente aberto às parcerias e às oportunidades da globalização"[100]. Segundo a mesma fonte, "de 2014 ao primeiro semestre de 2017, realizaram-se 140 ações de sensibilização do PSE, as quais abrangeram setecentas e vinte e nove (729) organizações nacionais e dois mil cento e oitenta e quatro (2184) indivíduos", salientando-se que, neste período, as "organizações que atuam nas áreas de Segurança e Defesa juntamente com Engenharia e Tecnologia, foram as mais visadas pelo Programa de Segurança Económica"[101].

No conjunto de políticas públicas aqui identificadas, assim como em outras anteriores, e em vigor, focadas em aspetos parciais da segurança no ciberespaço de que aqui não fizemos eco propositadamente por se desviarem um pouco do âmbito deste trabalho, e considerando o quadro nacional, parece não existir uma verdadeira coordenação politico-estratégica entre os diversos atores com responsabilidades no ciberespaço. Importa clarificar que esta perceção não questiona ou coloca em causa uma existente e comprovada coordenação operacional em matéria de investigação e reação nos espetros civil, judiciário, judicial e militar. Esta situação estará na génese, em Portugal, já desde há algum tempo, da proliferação de iniciativas conduzidas por entidades públicas e privadas que abordam a temática da cibersegurança de forma dispersa e avulsa[102], nem sempre de forma coordenada, e sem

[100] Fonte: https://www.sis.pt/pagina/63/programa-de-seguranca-economica, consultado em 27 de junho de 2018.

[101] *Ibidem*.

[102] Nesta área, apenas a título de exemplo, podem mencionar-se as conferências e a oferta formativa promovidas pelo CNCS ou pelo Instituto da Defesa Nacional (IDN), os eventos e debates promovidos pela Agência para a Sociedade do Conhecimento, IP (UMIC) e Fundação para a Ciência e a Tecnologia, IP (FCT) no âmbito da Sociedade da Informação e do Conhecimento, nomeadamente sobre a temática da Governação da Internet (cf. https://www.fct.pt/dsi/govinternet/iniciativaportuguesa.phtml.pt), as ações e iniciativas promovidas no âmbito do Centro Internet Segura (cf. http://www.internetsegura.pt/), as conferências promovidas por organizações de caráter privado, como a International Data Corporation (IDC) (cf. http://www.idcdx.pt/insights/idc-

que representem um evidente contributo determinante para os processos de decisão, isto é, para a definição de políticas estruturais, nomeadamente, de reformas estruturais[103] nesta matéria. Encontra-se, assim, um conjunto de medidas ad hoc, seja na realização de eventos e conferências, no estabelecimento de protocolos pontuais entre entidades públicas e privadas[104] e a academia no âmbito das competências técnicas necessárias para a mitigação das ameaças[105] ou em intervenções públicas sem que se consigam identificar mecanismos de operacionalização e acompanhamento da implementação da ENSC, uma situação que contraria o pressuposto do princípio de confiança mútua necessário nestas matérias, o que pode inviabilizar, por isso, e também aqui, a aplicação de verdadeiros processos de avaliação de políticas públicas.

events-2/) ou a COTEC Portugal (cf. http://imeetscyber.pt/), as conferências promovidas por instituições universitárias, entre muitos outros.

[103] Sobre reformas estruturais ver Amaral, 2014: 459.

[104] A Associação Portuguesa para o Desenvolvimento das Comunicações (APDC), no seguimento de um evento reservado que realizou, relata a existência de "57 protocolos [do CNCS] com entidades privadas" (APDC, 2018) – uma informação confirmada pelo GNS/CNCS em entrevista, em 11 de setembro de 2018. Acrescente-se ainda que estes protocolos, por norma, abrangem três áreas: a operacional (na resposta a situações e incidentes), a de ajudar as organizações a aumentar o seu grau de maturidade em termos de prevenção, deteção e reação, e a sensibilização de colaboradores através de pequenas sessões de apresentação.

[105] E.g. "Protocolos de Cooperação com entidades" (fonte: https://www.cncs.gov.pt/recursos/noticias/protocolos-de-cooperacao-com-entidades/ consultado em 12 de dezembro 2017), "Protocolo de colaboração com a Universidade do Porto" (fonte: https://www.cncs.gov.pt/recursos/noticias/assinatura-de-protocolo-de-colaboracao-com-a-universidade-do-porto/ consultado em 12 de janeiro de 2018).

IV. CONCLUSÕES E TRABALHO FUTURO

IV.1 Conclusões

> Assim, até mesmo aqueles que desejavam mais ardentemente libertar o Estado de todas as obrigações desnecessárias e cuja filosofia reclamava em todos os aspetos a limitação das atividades do Estado, não puderam fazer outra coisa que não fosse atribuir a esse mesmo Estado os novos poderes, órgãos e instrumentos requeridos pela instauração do *laissez-faire*.[106] (Polanyi, 2012: 311)

Partimos para este trabalho com uma pergunta que sabíamos de início ser de difícil resposta. Através do exercício de investigação que resultou na exposição anterior, procurámos encontrar as bases e os fundamentos que permitissem responder à pergunta "como poderão as empresas portuguesas, em especial as PME, lidar com os riscos de cibersegurança e, face ao quadro de políticas públicas nacional e internacional, que instrumentos têm ao seu dispor para tal?", bem como a outras proposições que aqui fomos apresentando.

Através das fontes a que tivemos acesso – bibliografia diversa sobre os temas relacionados com a transformação digital, entrevistas a peritos e entidades, públicas e privadas, e ainda dados disponíveis na Internet ou publicações, e aqui referimos também a dificuldade com que nos confrontámos sempre que, por natureza profissional, tivemos acesso a informação classificada que considerámos importante para a consolidação deste trabalho mas nos vimos forçados a descartar – foi-nos possível identificar um conjunto de dados que parece indiciar que as organizações em Portugal, e em especial as empresas de menor dimensão, ainda estão a lidar com os riscos de cibersegurança, ou riscos de segurança digital, de forma incipiente. Reconhecendo o valor e a pertinência das iniciativas conduzidas por algumas organizações e investigadores na tentativa de recolha de dados e informação sobre o quadro nacional, independentemente das suas motivações, salientamos, no entanto, que identificámos uma escassez de estudos e trabalhos que permitam o desenho desse quadro de forma coerente em matéria de comportamento das PME em relação aos riscos de segurança digital. Entre os que existem, dada a sua casualidade e diversidade metodológica nas abordagens ao tema, são poucas as pistas que encontram paralelo entre si, algumas mesmo entrando em aparente contradição.

Esta é uma situação que, no domínio das políticas públicas, se pode configurar de elevada importância e, nesse sentido, preocupante dada a necessidade de fundamentação para as políticas públicas e os processos de tomada de decisão. Mais ainda quando se trata de uma matéria que desperta alguma atenção junto dos cidadãos, como fica demonstrado em Correia, *et al*., em que "os inquiridos se encontram globalmente pouco satisfeitos com a ação do Estado em matérias de cibersegurança e cibercrime", sendo possível, através do modelo ali testado, "conjeturar quanto à existência de um enviesamento conjuntural das perceções no sentido de uma apreciação pouco objetiva da gestão pública e das políticas públicas nestas matérias" (2017: 107-108).

[106] Itálicos no original.

A ideia a que fomos conduzidos de que uma parte ainda significativa das organizações negligencia uma cultura de cibersegurança nos processos de transformação digital terá na sua génese dois fatores principais.

O primeiro fator será um eventual reflexo da incompreensão sobre o próprio processo de transformação digital. Um reflexo dessa incompreensão, que determina a concentração da responsabilidade destes processos quase exclusivamente nos departamentos de TIC, poderá resultar do facto de, como acredita a AP2SI, das " empresas onde esta situação acontece não entend[er]em o tema da transformação digital como um tema transversal à organização (com impacto ao nível dos recursos humanos, processos e modelos de negócio) mas como um tema puramente tecnológico"[107]. O mesmo entendimento que encontramos não só em outras entrevistas realizadas no âmbito deste trabalho, como nos diversos *fora* de discussão, públicos e privados, onde o tema encontra palco. Também para a COTEC Portugal, "o líder empresarial tem de perceber que [a cibersegurança] não é um problema da tecnologia ou do departamento de IT. É um problema de todas as áreas funcionais nomeadamente da gestão de processos de inovação nas empresas" (Monteiro, 2018).

O segundo fator, e sem que tenhamos possibilidade de aferir se em maior ou menor grau de influência na ação das empresas em relação ao primeiro, mesmo correndo o risco de parecer simplista, julgamos poder ser sintetizado numa frase: "a cibersegurança é uma chatice"[108]. Porque a "cibersegurança não é apenas uma questão técnica, mas um imperativo das organizações que implica gerir riscos visando a continuidade do negócio, protegendo os investimentos e os ativos, mantendo a reputação e vantagem competitiva" (Barbas e Sancho, 2018: 75), pode ser considerada uma "chatice" na medida em que a implementação e manutenção de uma cultura de cibersegurança nas organizações tem obrigatoriamente a ver com a cultura organizacional, o que implica, necessariamente, a realização de investimentos de ordem financeira ao nível da adaptação eficaz e eficiente de recursos – técnicos e humanos – e dos processos – por vezes dos próprios modelos de negócios das organizações – ao novo ambiente onde a informação passa a ser utilizada. Tendencialmente, as necessidades verificadas na implementação e manutenção de uma cultura de cibersegurança nas empresas, em linha com as orientações e boas práticas amplamente reconhecidas que aqui demos conta, são encaradas como uma despesa e não como um investimento.

Foi possível verificar que as organizações, e muito especialmente as empresas, têm atualmente disponível um leque variado de modelos, ferramentas, orientações e boas práticas que as pode guiar na implementação de mecanismos que lhes assegurem níveis de segurança elevados, permitindo o seu funcionamento com níveis de risco de segurança digital que possam considerar aceitáveis (ITI, 2011; Kriz, 2011; OCDE, 2015a; Rosenquist, 2015; Teodoro, *et al*., 2015; Paulsen, 2016; Paulsen e Toth, 2016a; Berven, 2016; BBB, 2017; Bell, 2017; GNS, 2018a; Daniels; 2017; ENISA, 2017a; FERMA, 2017; Paul, 2017; Stanton, *et al*., 2017; Stark, 2017; Dietzel, 2018).

[107] Resposta da AP2SI em entrevista escrita.

[108] Caracterização utilizada por um investigador numa entrevista realizada em 30 de maio de 2018.

A implementação destes modelos, ferramentas, orientações e boas práticas terá, necessariamente, de levar em consideração a especificidade de cada organização – dimensão, modelo de negócio, produtos e serviços, processos, clientes, fornecedores, etc. – devendo ser orientada por modelos e avaliações de investimento cuidadosas na área da sua proteção e segurança (Gordon e Loeb, 2002; 2015; 2016; Anderson e Moore, 2006; Rowe e Gallaher, 2006; Böhme, 2010; Etzioni, 2011; Mukhopadhyay, *et al*., 2013; Hutchins, *et al*., 2015; DeSmit, *et al*., 2016; Lam, 2016; Mayadunne, 2016; Nagurney e Shukla, 2017; Alali, *et al*., 2018; Chronopoulos, *et al*., 2018; Weishäupl, *et al*., 2018).

Nesta panóplia de opções, e considerando como de enorme relevância o trabalho desenvolvido pela OCDE (2015a) no sentido de disponibilizar princípios e orientações sobre a gestão de risco de segurança digital a todas as partes interessadas, com uma clara distinção entre o papel e a responsabilidade de cada uma, onde se incluem, naturalmente, as empresas, e a partir do qual algumas associações internacionais definiram recomendações de modelos de governação do risco de segurança digital (FERMA, 2017), julgamos importante destacar um relatório produzido pela ENISA em novembro de 2017 que pode constituir uma valiosa contribuição para a implementação desses princípios e orientações. Este relatório, que no nosso entender responde igualmente aos nove elementos preconizados pela ONU, em 2002, para o estabelecimento de uma cultura de cibersegurança[109], tem como objetivo o de "auxiliar na promoção da compreensão e adoção de programas de CSC [cultura de cibersegurança] dentro das organizações" e resulta de contributos retirados de "múltiplas disciplinas, incluindo ciências organizacionais, psicologia, direito e cibersegurança" (ENISA, 2017a: 5). Dado que aborda conceptualmente questões relacionadas com as organizações, requisitos e comportamentos com vista à construção de culturas de cibersegurança, apresenta-se como uma ferramenta acessível às empresas para um maior aprofundamento do entendimento e implementação de boas práticas essenciais para minimizar os riscos de segurança digital a que estão expostas nesta era da transformação digital. Nele é sugerida a implementação de uma cultura de cibersegurança nas organizações em oito etapas como se mostra no quadro 4.1.

[109] No anexo da Resolução 57/239 da Assembleia Geral são estabelecidos nove elementos "para criar uma cultura de cibersegurança global", a saber: sensibilização, responsabilidade, resposta, ética, democracia, avaliação do risco, desenho e implementação de segurança, gestão da segurança e, por fim, reavaliação (ONU, 2003: 2-3).

Quadro 4.1 – Etapas para a implementação de uma cultura de cibersegurança nas organizações

Etapa	Ação a implementar
1.ª	Definir e estabelecer o núcleo do trabalho de grupo que definirá a estratégia e a política de cibersegurança e supervisionará a sua implementação
2.ª	Conhecer e avaliar os riscos na organização através do conhecimento extraído do envolvimento de todas as pessoas e áreas funcionais da organização (culturas, práticas, processos, etc.)
3.ª	Definir os principais objetivos a atingir, assim como os critérios que avaliam o sucesso e o público-alvo
4.ª	Identificar a situação atual da organização e analisar o hiato entre essa situação e aquela que se pretende atingir (definida na etapa anterior)
5.ª	Identificar e selecionar as atividades necessárias para eliminar ou reduzir o hiato identificado na etapa anterior
6.ª	Pôr em curso, cada uma individualmente e depois em simultâneo, as atividades identificadas na etapa anterior por forma a avaliar o seu impacto na organização
7.ª	Repetir o processo de identificação da situação atual da organização por forma a ser possível avaliar o impacto da cultura de cibersegurança na organização
8.ª	Rever e considerar os resultados e as experiências obtidas nestas etapas anteriores por forma a permitir reavaliar a estratégia da organização em matéria de cibersegurança e do seu modelo de negócio

Legenda: quadro com oito etapas para a definição e implementação de uma cultura de cibersegurança nas organizações (fonte: ENISA, 2017a)

Importa referir que uma cultura de cibersegurança nas organizações é tão mais eficaz quanto maior for a periodicidade com que é revista, reavaliada e atualizada: "[…] modificar o comportamento dos trabalhadores e o conjunto da cultura de cibersegurança dentro das organizações é um processo contínuo" (ENISA, 2017a: 13).

Num quadro democrático em que se poderiam levantar algumas reservas na regulação da atividade das empresas[110] e em que as relações económicas e sociais se desmaterializam passando a

[110] Reservas que habitualmente são colocadas por autores, ou ideólogos, cuja teoria económica assenta na ideia do "livre" funcionamento dos mercados. Relativamente ao "livre funcionamento dos mercados", ainda que sem

ocorrer, cada vez mais, em ambientes digitais, perante a constatação de "que em Portugal ainda não se atingiu um estado de maturidade de cultura de segurança económica como o existente noutros Estados ocidentais"[111], tornam-se imprescindíveis, portanto, quadros normativos de referência. Isto é, a definição, implementação e monitorização de políticas públicas robustas e orientadoras por forma a "garantir a não exclusão dos indivíduos e organizações do ciberespaço, o que passa não apenas pela sua educação para o exercício de uma "cidadania digital", mas, sobretudo, pela garantia de acessos seguros aos meios e sistemas de informação, assim como pela proteção da privacidade." (Paulo Moniz em Nunes, 2018: 20).

Neste campo, Portugal saiu de um estado de inércia – ou de uma inércia do Estado? – que praticamente se verificava em matérias estratégicas para o, e no, ciberespaço com a adoção, em 2015, da ENSC, sendo que até aí alguns dos aspetos relacionados com a segurança no ciberespaço, o cibercrime ou a ciberdefesa eram, e continuam ainda a ser em alguns casos, como anteriormente fizemos referência, pela sua natureza, atendidos por regulamentação isolada e específica. A ENSC surgiu, assim, como um instrumento estratégico "com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento de sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio" (Presidência do Conselho de Ministros, 2015), mas com notórias deficiências ao nível da sua operacionalização – desde logo pela inexistência de um plano de ação que permita uma identificação inequívoca de papéis e responsabilidades de todas as partes interessadas na implementação desta estratégia nacional. Falha, assim, na conceção da arquitetura de cibersegurança, um dos seis fatores mínimos identificados em Barbas e Sancho, para o desenvolvimento de políticas públicas nesta matéria: "[…] o quadro no qual se relacionam os organismos envolvidos na cibersegurança de um país, a forma como se relacionam e as funções atribuídas a cada um deles, é o que permite identificar a arquitetura de cibersegurança de um país. Com efeito, refere-se aos órgãos e entidades nacionais ou setoriais que compõem o sistema nacional de cibersegurança e a interação existente entre eles" (Barbas e Sancho, 2018: 57).

Posteriormente, a Resolução de Conselho de Ministros n.º 115/2017 estabeleceu a criação de um Conselho Superior de Segurança do Ciberespaço (CSSC), entretanto revogada pela Lei n. 46/2018, cujo objetivo primeiro, entre outros, era o de "assegurar a coordenação político-estratégica para a segurança do ciberespaço" (Presidência do Conselho de Ministros, 2017) mas com uma configuração que nos parecia enviesada pela sua composição de carácter exclusivamente[112] público quando esta coordenação político-estratégica, segundo a ENSC, dependerá certamente da ação do setor privado uma vez que reconhece que "grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida por operadores privados, a quem cabe a responsabilidade primária pela sua proteção" (Presidência do Conselho de Ministros, 2015). Um enviesamento que continuamos a identificar na Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do

---

espaço para essa discussão, colocamos acentuadas reservas quanto à "liberdade" que se diz existir (cf. Chang, 2002; 2010; 2014; Polanyi, 2012; Mazzucato, 2018).

[111] Fonte: https://www.sis.pt/pagina/63/programa-de-seguranca-economica, consultado em 27 de junho de 2018.

[112] Ver a observação que fizemos no Capítulo III sobre a composição deste CSSC.

Ciberespaço, transpondo a Diretiva (UE), e, mantendo o seu objetivo politico-estratégico, introduz alterações à composição do CSSC em relação à formação inicial de 2017, mesmo considerando as alterações introduzidas pela Assembleia da República durante o processo de apreciação parlamentar[113]. Por essa razão, mesmo que o processo em curso de revisão e preparação de uma nova versão da ENSC assuma, aparentemente, uma característica mais inclusiva e participada no que respeita ao setor privado, "onde a aposta foi alargar o debate a todos os intervenientes dos setores público e privado" (APDC, 2018), depreendendo-se pelos objetivos macro tornados públicos que se pretende uma maior articulação e colaboração entre a academia, o setor privado e o setor público (APDC, 2018), esta participação não encontrará seguramente continuação no momento da coordenação político-estratégica da ENSC, da sua monitorização ou avaliação. Considera o GNS/CNCS[114], que reconhece e partilha desta preocupação por nós levantada, que a questão poderá ser, de alguma forma, minimizada pela participação no CSSC de representantes da tutela da Economia, como o IAPMEI, ou pela rede nacional de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT).

Sendo que consideramos perniciosa a cópia de modelos sem uma devida atenção ao enquadramento e contexto em que são aplicados, em matéria de governação da estratégia de cibersegurança julgamos que, apesar das muitas similitudes encontradas em matéria de objetivos e competências, algumas das práticas identificadas noutros modelos seguidos internacionalmente ao nível de representação dos diversos setores, como no caso dos Países Baixos, poderiam igualmente encontrar reflexo no modelo seguido em Portugal. Ou seja, tal como nos Países Baixos, o órgão com competências de coordenação, monitorização e avaliação da sua implementação – em Portugal o CSSC – poderia assumir uma maior representatividade com a participação direta de empresas – grandes, PME e operadores de infraestruturas críticas – ou de associações representativas, e da academia, através de universidades, institutos politécnicos e de centros de investigação: "com estas

[113] Sobre a composição do CSSC, e apesar da Proposta de Lei n.º 119/XIII/3.ª que estabelece o regime jurídico da segurança do Ciberespaço alargar mais a sua composição em relação à composição inicialmente adotada pela Resolução de Conselho de Ministros n.º 115/2017, a Lei n.º 46/2018, de 13 de agosto, que resultou da discussão na especialidade na AR inclui "dois deputados designados pela Assembleia da República através do método de Hondt", de "um representante da área da administração eleitoral" em vez de "um representante da área da administração interna", e também representantes dos governos das Regiões Autónomas dos Açores e da Madeira – um por cada RA. No entanto, deve atender-se ao facto da Lei n.º 46/2018 ter revogado a Resolução do Conselho de Ministros n.º 115/2017 sem que tivesse mantido outras atribuições ao CSSC nomeadamente em termos de competências atribuídas. Por exemplo, se a anterior redação estabelecia "que, a convite do/a presidente, podem ainda participar nos trabalhos do CSSC representantes indicados por outras entidades, bem como personalidades de reconhecido mérito na área em que são desenvolvidos os trabalhos" (Presidência do Conselho de Ministros, 2017), a nova redação estabelece que "o presidente, por sua iniciativa ou a pedido de qualquer dos membros do Conselho, pode convocar outros titulares de órgãos públicos ou convidar outras personalidades de reconhecido mérito para participar em reuniões do Conselho Superior de Segurança do Ciberespaço" (Assembleia da República, 2018b) – parece, assim, atendendo às competências atribuídas ao CSSC, passar-se de um cenário em que outras entidades poderiam "participar nos trabalhos do CSSC" para um em que apenas passam a "participar em reuniões".

[114] Em entrevista em 11 de setembro de 2018.

diferentes perspetivas e portfólios, a composição do Conselho [de Cibersegurança dos Países Baixos] também equilibra os vários interesses e tópicos nacionais relevantes para a cibersegurança, além da óbvia combinação público-privada" (Kaska, 2015: 11)[115].

Já a questão que levantámos anteriormente sobre a ausência de um plano de ação com uma clara identificação dos responsáveis pela sua implementação em prol da segurança do ciberespaço parece, de alguma forma, respondida também pelo processo de revisão da ENSC que se encontra atualmente a decorrer, dado que "a nova estratégia estabelece que terá que ser definido um plano de ação até 120 dias da publicação do documento" (APDC, 2018), o que poderá indiciar uma menor problemática, no futuro, na operacionalização da ENSC.

IV.2. Proposta de trabalho futuro

Admitindo o pressuposto de que "a regulamentação deve-se focar no estabelecimento de requisitos mínimos de segurança tecnológica, na exigência do levantamento de capacidades de monitorização, deteção e reação, mas, também, na educação dos cidadãos para a cibersegurança" (Paulo Moniz em Nunes, 2018: 23), e num plano em que "Portugal tem a clara ambição de liderar, até 2030, a área do digital" [*sic*] (LUSA, 2018), a nossa proposta é a de que se torna de elevada importância que o Estado assuma um papel que vá para além da simples regulação e regulamentação. Que tenha um papel mais ativo e interventivo na criação das condições para a implementação de culturas de cibersegurança. Ou seja, da mesma forma que o conjunto de políticas públicas que tem vindo a ser implementado em Portugal prevê um reforço dos incentivos políticos e financeiros para a transformação digital, deve também prever incentivos e estímulos, de natureza diversa, para a construção e implementação de culturas de cibersegurança nas organizações em Portugal, e muito em especial, nas empresas.

Atendendo ao exemplo do Regulamento Geral sobre a Proteção de Dados (RGPD), que passou a vigorar a partir de 25 de maio de 2018 (JOUE, 2016)[116], em que temos claramente uma ação por via da regulamentação e a ação do Estado português terá incidido, essencialmente, em iniciativas de disseminação e esclarecimento[117] sobre a sua aplicação[118], num estudo desenvolvido pela LCG -

[115] Importa mencionar que, em abril de 2018, o Governo dos Países Baixos lançou uma nova Agenda Nacional de Cibersegurança que, neste campo, prevê o reforço de parcerias entre o setor público e o privado através da criação de redes de parcerias público-privadas e o estabelecimento de uma "aliança" nacional entre organizações. Cf. "National Cyber Security Agenda – A cyber secure Netherlands", disponível em https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf, consultado em 13 de agosto de 2018.

[116] O RGPD "coloca nas organizações públicas e privadas o ónus da responsabilidade da proteção de dados, acrescenta inevitavelmente obrigações que têm um impacto considerável nas suas operações" (IAPMEI, 2018: 2) com "alterações significativas ao nível das regras do jogo e da operacionalização destes princípios" (KPMG, 2017: 2).

[117] A este propósito, importa destacar as iniciativas conduzidas pelo IAPMEI mas também a disponibilização pelo Gabinete Nacional de Segurança (GNS) de um manual de boas práticas "RGPD e a Segurança das Redes e

Consultoria, S.A. em parceria com o IAPMEI é possível observar que das mais de mil empresas inquiridas[119], apenas 8% "considera ter todas as medidas adequadas para responder às exigências do regulamento" e 49% "afirmam estar parcialmente preparadas" (IAPMEI, 2018: 6). Note-se que, segundo um estudo da KPMG, e atendendo ao impacto que o regulamento da UE tenderá a provocar nas organizações[120], cerca de um ano antes da sua aplicação, a percentagem das organizações inquiridas que diziam não ter sequer começado "a implementar medidas efetivas para garantir a conformidade com o RGPD" (KPMG, 2017: 5) era ainda cerca de 85%.

Considerando

i) a enorme dependência de ambientes digitais para o funcionamento da sociedade, em todas as áreas;

ii) a importância que a segurança representa para o correto, eficaz e eficiente funcionamento desses ambientes;

iii) que a transformação digital continuará a decorrer por muito tempo, criando fatores de disrupção na economia, na sociedade e nas políticas dos governos (OCDE, 2017b: 26);

iv) que "o ciberdomínio é a um tempo um ambiente artificial novo e volátil" (Nye, Jr., 2012: 173) e, por essa razão, "os governos serão forçados a mudar a sua abordagem quando se trata da criação, revisão e aplicação de regulamentação" (Schwab, 2017a: 66);

v) a inexistência de estudos regulares e alargados que permitam identificar e mapear um quadro nacional em matéria de cibersegurança, limitando, assim, o apoio e a fundamentação na tomada de decisão atendendo a que "o desenho de melhores políticas para a economia e sociedade digital requer, não só melhor conhecimento sobre as mudanças tecnológicas em curso, mas também mais esforços para melhorar a medição, as evidências e as análises" (OCDE, 2017b: 26); e

---

Sistemas de Informação" considerando que o "RGPD vem, assim, exigir uma atenção cuidada às organizações que lidam com dados pessoais, obrigando à implementação de práticas e salvaguardas suplementares, bem como a repensar a forma como se encara a segurança da informação e das redes e sistemas de informação" (GNS, 2018: 3).

[118] Por se tratar de um regulamento da UE, a sua aplicação é direta não carecendo de transposição, o que não inviabiliza que os Estados-Membros tenham de adotar legislação secundária tendo em vista o seu cumprimento (cf. Matos, 2015). No caso português, a aplicação do RGPD implica a revogação e alteração de diplomas legislativos relacionados com a proteção de dados, um processo em curso na Assembleia da República (Reis, 2018).

[119] Os valores no Relatório são sempre apresentados em percentagens pelo que não é preciso o valor absoluto a que corresponde o "mais de mil empresas" – pela comunicação social ficamos a saber que serão "cerca de 1.500 empresas" (Fernandes, 2018). Não deixa também de ser significativo que estas "mais de mil" respostas resultam de um inquérito lançado a "cerca de 20.000 empresas" (IAPMEI, 2018: 5).

[120] Há mesmo relatos na comunicação social que dão conta desse impacto como o da notícia veiculado pelo jornal Economia Online de que "Startup portuguesa fecha [*sic*]. Não é capaz de cumprir RGPD" (ECO e Patrício, 2018).

vi) à responsabilidade dispersa e transversal a várias entidades e uma falta de clareza quanto ao papel que desenvolvem no âmbito da cibersegurança,

estamos convictos que em Portugal não existe outra forma de desenvolver e definir estratégias robustas que atendam a todos os interesses legítimos, preocupações e desafios que a área da cibersegurança coloca, senão com um forte envolvimento do Estado e uma necessária coordenação da responsabilidade deste no envolvimento, em todas as fases do ciclo das políticas públicas, dos diversos setores da sociedade: o setor privado, o setor público nos seus diversos níveis, a academia e a sociedade civil.

Este modelo de governação na definição, implementação e monitorização de regulamentação e estratégias, por se acreditar que é o que melhor poderá fazer o alinhamento de preocupações, objetivos e prioridades, salvaguardando a partilha de responsabilidades e limitando as situações de captura de determinadas tomadas de decisão em função de interesses isolados, terá de ser, forçosamente, incorporado nos mecanismos que asseguram a implementação destas iniciativas.

Para esse efeito, uma Estratégia Nacional de Segurança do Ciberespaço, que compreende diversos níveis de abordagem e de operacionalização, deveria contemplar uma estrutura na dependência direta do Estado com capacidade de trabalhar e se articular não só ao nível das diversas áreas políticas mas também com estruturas similares e complementares noutros domínios da sociedade, públicas e privadas, capaz de fomentar ativamente a produção de novo conhecimento em cibersegurança, incluindo nos aspetos tecnológicos, normativos e ao nível das competências necessárias para a sua implementação, como, por exemplo, na definição de orientações e requisitos para programas científicos e tecnológicos de I&D e de educação nos diversos níveis de ensino. Esta estrutura teria de ter também a capacidade para, em conjunto com outras entidades responsáveis nessa matéria, proceder a estudos e inquéritos regulares do quadro nacional nesta área, por forma a melhor suportar e apoiar os decisores públicos e a produção de relatórios de avaliação regulares. Deveria ainda dispor de recursos e competências que, em colaboração com outras entidades públicas e privadas, ou isoladamente sempre que não conseguisse encontrar nas anteriores as necessárias valências, lhe permitisse prestar serviços técnicos, de forma pontual ou planeada, às organizações nas vertentes de capacitação tecnológica, organizacional e humana, independentemente da sua tipologia e especificidades, contribuindo assim, não só para o estabelecimento de redes de confiança, como para a sensibilização, desenvolvimento e implementação de uma cultura de cibersegurança nas organizações.

Certos do risco que esta proposta corre, uma vez que as discussões que impliquem a dimensão e/ou as áreas de intervenção do setor público, seja ao nível social ou ao nível económico[121], são habitualmente marcadas mais "por visões políticas e posições ideológicas do que informada[s] por evidências científicas profundas" (Mazzucato, 2018: 11), entendemos que é uma proposta que carece, necessariamente, de uma reflexão mais aprofundada e multidisciplinar. A sua abrangência requer que

[121] Sobre este tema e a sua relação com o valor que decorre para a economia da intervenção e a ação do setor público ver Mazzucato, 2018: 229-269.

seja feita uma avaliação de todas as implicações não só ao nível organizacional e funcional, como também ao nível de dispositivos jurídicos, ainda que, neste campo, e confessando as nossas limitações nesta disciplina, não encontremos, à partida, uma necessidade de grandes modificações.

No entanto, este não será um modelo totalmente disruptivo dado que o que aqui expusemos encontra, em alguns aspetos, determinados paralelismos com o que foi implementado em termos de estratégias para a transformação digital e de cibersegurança em diversos Estados-Membros da UE, e.g. nos Países Baixos ou no Reino Unido, que, tal como Portugal, se veem na obrigação de seguir um conjunto de normativos jurídicos provenientes da UE. Com as devidas cautelas devido ao fator regional existente na Alemanha, tivemos ainda como referencial, a instalação e funcionamento de centros para apoiar especificamente as PME nos processos de transformação digital no âmbito do programa nacional de digitalização da indústria, aproveitando a transferência de tecnologia através da prestação de serviços de apoio ao nível da disseminação e esclarecimento, formação específica e à medida, ambientes de testes e experimentação e implementação de projetos (Müller e Hopf, 2017). Dado que Portugal também já possui instrumentos de proximidade com um "conjunto de produtos e serviços que visam um acompanhamento personalizado, e na transferência e partilha de conhecimento e de informação útil aos empresários e investidores"[122] através do IAPMEI, não se revelaria de muita dificuldade o aproveitamento desta capacidade já instalada através do aprofundamento da articulação entre esta rede e uma estrutura como a que anteriormente propusemos.

Mais ainda, uma estrutura desta natureza poderia responder aos desafios lançados pela UE em matéria de reforço da cibersegurança que prevê o estabelecimento ao nível europeu de "uma rede de centros de competências em matéria de cibersegurança[123] constituída em torno de um Centro Europeu de Investigação e de Competências em matéria de Cibersegurança" (Comissão Europeia, 2017: 10). A recente proposta da Comissão Europeia para a criação do Programa Europa Digital é, porventura, uma das evidências com maior relevância da aposta que a UE continua a fazer nesta área da cibersegurança e das competências – tecnológicas e humanas – necessárias para o funcionamento, em segurança, do mercado único digital, dado que estabelece como ponto de partida negocial cerca de 2 mil milhões de euros[124] de financiamento para o objetivo específico "Cibersegurança e confiança"[125] (Comissão Europeia, 2018: 29).

---

[122] Fonte https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Assistencia-Tecnica-e-Formacao.aspx, consultado em 15 de julho de 2018.

[123] "A rede deverá incluir centros existentes e futuros dedicados à cibersegurança, criados nos Estados-Membros, cujos membros serão, em princípio, organizações e laboratórios de investigação públicos" (Comissão Europeia, 2017: 10).

[124] 1 998 696 000 Euros.

[125] Neste objetivo específico, pretende-se que a intervenção financeira vise "apoiar, em conjunto com os Estados-Membros, a aquisição de equipamentos avançados de cibersegurança e de ferramentas e infraestruturas de dados em plena conformidade com a legislação relativa à proteção de dados; apoiar a melhor utilização possível dos conhecimentos, capacidades e competências da Europa no domínio da cibersegurança; assegurar uma implantação alargada das mais recentes soluções em matéria de cibersegurança em todos os

Este modelo que propomos à avaliação está longe de querer assumir a existência de uma estrutura agregadora ou centralizadora da produção de conhecimento, operacionalização ou elaboração de políticas públicas em matéria de cibersegurança. Esta estrutura assumir-se-ia como uma estrutura charneira com outras entidades e organizações, públicas e privadas, e com um modelo de governação participado e alargado. Dessa forma, uma vez assegurados os mecanismos de fundamentação que anteriormente descrevemos, desde a avaliação de necessidades e de capacidades até à avaliação de impacto produzido pelas políticas públicas[126], e tendo em conta a ideia de que os processos de decisão nesta área são habitualmente "caracterizados por uma falta de transparência e responsabilização" (Bendiek, 2012: 24, citado em Carrapico e Barrinha, 2017: 1268), acreditamos que os processos de decisão e definição de políticas públicas sairiam, seguramente, bastante reforçados. Com este modelo pressupõe-se que o Estado mais facilmente possa exercer aquilo que Joseph S. Nye, Jr. define como "poder inteligente", isto é "a combinação do poder duro da coerção e do pagamento com o poder suave da persuasão e da atração" (Nye, Jr., 2012: 14).

No que respeita a políticas públicas, e também se aplica às em matérias de cibersegurança, a sua implementação não deve ficar limitada pela regulamentação imposta pelo setor público e pela autorregulação que se espera e exige ao setor privado. Face ao quadro atual de exigências sociopolíticas e a ambição nacional colocada nas estratégias de inovação, investigação e desenvolvimento e, em especial, pelo grande enfoque no digital, acreditamos que uma proposta como aquela que aqui deixamos, também por se considerar que "o papel do setor público aqui não é apenas o da diminuição do risco e equilíbrio da concorrência mas o de inclinar o campo de atuação em direção aos objetivos desejados – criar e moldar os mercados o que aumenta as expetativas das empresas sobre oportunidades futuras de crescimento motivando, assim, o investimento privado" (Kattel e Mazzucato, 2018: 2), permitirá colocar o Estado numa posição de assumir ainda mais a sua centralidade no sistema de inovação (Nelson, 2017) e de melhor cumprir a missão que lhe está confiada em termos de segurança e proteção. Face à necessidade de uma implementação de políticas públicas capazes de responder aos desafios atuais e futuros impostos, também, pela transformação digital, uma abordagem deste género, tendo em vista a inovação, poderá melhor capacitar o Estado para "liderar e aprender"[127] em vez de este ficar limitado ao tradicional posicionamento do setor público na implementação de instrumentos para colmatar as falhas de mercado[128] e posterior avaliação do seu impacto nos restantes setores, isto é, no papel de "apoiar e medir"[129] (Kattel e Mazzucato,2018): "o desenho de uma boa política pública é, em grande parte, o desenho de uma estrutura organizacional

---

setores da economia; reforçar as capacidades dos Estados-Membros e do setor privado a fim de ajudar a assegurar o cumprimento da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União" (Comissão Europeia, 2018: 27).

[126] Sobre avaliação de políticas públicas ver HM Treasury, 2011.

[127] "Lead-and-learn" (Kattel e Mazzucato, 2018).

[128] Sobre as falhas de mercado ver Nelson, 2017; Kattel e Mazzucato, 2018; Mazzucato, 2018.

[129] "Support-and-measure" (Kattel e Mazzucato, 2018).

capaz de aprender e de ajustar o comportamento em resposta ao que aprendeu" (Nelson e Winter, 1982 citado em Kattel e Mazzucato, 2018: 9).

Em pleno debate sobre a criação de valor na economia que resulta da ação do Estado (Mazzucato, 2018: 229-269), e para o qual aspirámos modestamente contribuir, nesta matéria há, concomitantemente, um outro papel que o Estado não deve demitir-se de desempenhar, seja em termos tecnológicos, seja em termos humanos: o de liderar pelo exemplo.

BIBLIOGRAFIA

A.A.K. (2013), "How did Estonia become a leader in technology?", *The Economist* (online), 31 de julho.
Disponível em: https://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21?fsrc=scn/fb/te/bl/ed/howdidestoniabecomealeaderintechnology (consultado em 28 de setembro 2013).

Afonso, Magalhães (2018), "Empresas europeias ainda longe da transformação digital", *Jornal i*, 29 de janeiro, p. 9.

Ahmad, Nadim e Paul Schreyer (2016), "Measuring GDP in a Digitalised Economy", *OECD Statistics Working Papers*, 2016/07, OECD Publishing, Paris.
Disponível em: http://dx.doi.org/10.1787/5jlwqd81d09r-en

Alali, Mansour, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab A.L. Rassan e Md Zakirul Alam Bhuiyan (2018), "Improving risk assessment model of cyber security using fuzzy logic inference system", *Computers & Security*, 74, May, pp. 323–339.
Disponível em:https://www.sciencedirect.com/science/article/pii/S0167404817302006 (consultado em 18 de abril 2018)

Amaral, Diogo Freitas do (2014), *Uma Introdução à Política*, Lisboa, Bertrand Editora.

Anderson, Chris (2017), *A Cauda Longa*, Lisboa, Actual Editora.

Anderson, Ross e Tyler Moore (2006), "The Economics of Information Security", *Science 314 (5799)*, pp. 610–613.
Disponível em: http://dx.doi.org/10.1126/science.1130992

Angwin, Júlia (2015), *Dragnet Nation*, New York, St. Martin's Griffin.

AP2SI (2016), *Inquérito Aberto à Segurança da Informação nas Instituições em Portugal,* 1.ª edição.
Disponível em: https://ap2si.org/inquerito/resultados-2015/.

APDC (2018), "Evento APDC – Jantar reservado APDC debate cibersegurança nacional".
Disponível em: http://www.apdc.pt/iniciativas/agenda-apdc/jantar-reservado-apdc-debate-ciberseguranca-nacional (consultado em 11 de julho 2018).

Assembleia da República (2018), *Lei n.º 46/2018 - Diário da República n.º 155/2018, Série I de 2018-08-13, que Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*.
Disponível em: http://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html.

Bailey, Tucker, Brian Kolo, Karthik Rajagopalan e David Ware (2018), *Insider threat: The human element of cyberrisk*, setembro.
Disponível em: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk (consultado em 26 de setembro 2018).

Baller, Silja, Soumitra Dutta e Bruno Lanvin (2016), *The Global Information Technology Report 2016 – Innovating in the Digital Economy*, Geneva, World Economic Forum.
Disponível em: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

Barbas, João e Carolina Sancho (2018), "Cibersegurança e Políticas Públicas: Análise Comparada dos Casos Chileno e Português", *IDN Cadernos 29*, Instituto da Defesa Nacional.
Disponível em: https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_29.pdf.

BBB (2017), *2017 State of Cybersecurity Among Small Businesses in North America*.
Disponível em: https://bbbprograms.org/siteassets/documents/bbb-cybersecurity/cybersecurity_final_lores.pdf (consultado em 1 de junho 2018).
BBC (2017), "Personal details of nearly 200 million US citizens exposed", *BBC* (online), 19 de junho.
Disponível em: https://www.bbc.com/news/technology-40331215 (consultado em 19 de setembro 2018).
BBC (2017a), "Massive Equifax data breach hits 143 million", *BBC* (online), 8 de setembro.
Disponível em: https://www.bbc.com/news/business-41192163 (consultado em 19 de setembro 2018).
BBC (2018), "Cyber attack led to Bristol Airport blank screens", *BBC* (online), 16 de setembro.
Disponível em: https://www.bbc.com/news/uk-england-bristol-45539841 (consultado em 19 de setembro 2018).
BBC (2018a), "Equifax fined by ICO over data breach that hit Britons", *BBC* (online), 19 de setembro.
Disponível em: https://www.bbc.com/news/technology-40331215 (consultado em 19 de setembro 2018).
Bell, Shane (2017), "Cybersecurity is not just a 'big business' issue", *Governance Directions*, 69 (9), October, pp. 536–539.
Disponível em: https://www.mcgrathnicol.com/app/uploads/cybersecurity-sme-october-2017.pdf (consultado em 8 de novembro 2017)
Bernardo, Luís (2018), "A sociedade da segurança estatística", *Le Monde Diplomatique – Edição Portuguesa*, Maio, pp. 8-9.
Berven, Mark (2016), "Cybersecurity poses a serious threat", *Smart Business Columbus*, 25 (3), December, p. 12 (consultado via b-on.pt em 8 de novembro 2017)
Bobbio, Norberto, Nicola Matteucci e Gianfranco Pasquino (2004), *Dicionário de Política Vol. 1,* 12.ª edição, Brasília, Editora Universidade de Brasília.
Böhme, Rainer (2010), "Security Metrics and Security Investment Models", em Echizen I., Kunihiro N., Sasaki R. (eds) *Advances in Information and Computer Security*. *IWSEC 2010. Lecture Notes*, Computer Science, 6434, Berlin, Heidelberg, Springer.
Disponível em: https://www.is.uni-muenster.de/security/publications/Boehme2010_SecurityInvestment-IWSEC.pdf (consultado em 30 de maio 2018).
Borges, João Vieira e Teresa Ferreira Rodrigues (2016), *Ameaças e Riscos Transnacionais no Novo Mundo Global*, Porto, Fronteira do Caos Editores.
Bower, Joseph L. e Clayton M. Christensen (1995), "Disruptive Technologies: Catching the Wave", *Harvard Business Review 73*, 1, pp. 43–53.
Disponível em: https://hbr.org/1995/01/disruptive-technologies-catching-the-wave (consultado em 03 de fevereiro 2018).
Brangetto, Pascal (2015), *National Cyber Security Organisation: France*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
Brynjolfsson, Erik e Brian Kahin (2000), *Understanding the Digital Economy: Data, Tools, and Research* , Cambridge, The MIT Press.
Butrimas, Vytautas (2015), *National Cyber Security Organisation: Lithuania*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Canadian Institute of Actuaries, Casualty Actuarial Society e Society of Actuaries (2017), *Cybersecurity: Impact on Insurance Business and Operations*.
Disponível em: https://www.casact.org/community/sections/rms/JRMS_cyber_security_essays%20EN.pdf (consultado em 26 de outubro 2017).

Cardoso, Gustavo, Ana Rita Coelho, António Firmino da Costa, André Pereira (2015), *A Sociedade em Rede em Portugal – Uma década de transição*, Coimbra, Almedina.

Cardoso, Margarida G.M.S., Rosário D. Laureano e Carlos Serrão (2017), "Cybersecurity culture in Portuguese organizations: an exploratory analysis", *International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC)*, 4 (2), pp. 23–30.
Disponível em: http://www.uajournals.com/ijisebc/images/papers/2017/4/2/3.pdf (consultado em 16 de maio 2018).

Carrapico, Helena e André Barrinha (2017), "The EU as a Coherent (Cyber)Security Actor?", *Journal of Common Market Studies*, 55 (6), pp. 1254–1272.
Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12575 (consultado em 16 de janeiro 2018).

Carvalho, Luís Nandin de (2000), *Direito ao Lobbying, Teorias, meios e técnicas*, Lisboa, Edições Cosmos.

Castells, Manuel (2011), *A Era da Informação: Economia, Sociedade e Cultura – Volume I – A Sociedade em Rede*, Lisboa, Fundação Calouste Gulbenkian.

Glorioso, Ludovica (2015), *National Cyber Security Organisation: Italy*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Cendoya, Alexander (2016), *National Cyber Security Organisation: Spain*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Center for Cyber Safety and Education e $(ISC)^2$ (2017), *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*, London, Crown.
Disponível em: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf (consultado em 09 de junho 2018)

Cerf, Vinton G. (2013), "Revisiting the Tragedy of the Commons", *Communications of the ACM*, Vol. 56, 10, p. 7.
Disponível em: https://cacm.acm.org/magazines/2013/10/168181-revisiting-the-tragedy-of-the-commons/fulltext (consultado em 18 de janeiro 2018).

Chagnollaud, Dominique (1999) (dir), *Dicionário da vida política e social*, Lisboa, Plátano Edições Técnicas.

Chang, Ha-Joon (2002), "Breaking the Mould: An Institutionalist Political Economy Alternative to the Neoliberal Theory of the Market and the State". Cambridge Journal of Economics, 26, 539-559.

Chang, Ha-Joon (2010), *23 Things They Don't Tell You About Capitalism*, London, Penguin Books.

Chang, Ha-Joon (2014), "Economics: A User's Guide". London: Penguin.

Christensen, Clayton M., Michael E. Raynor e Rory McDonald (2015), "What Is Disruptive Innovation?", *Harvard Business Review*, December, pp. 44–53.
Disponível em: https://hbr.org/2015/12/what-is-disruptive-innovation (consultado em 03 de fevereiro 2018).

Chronopoulos, Michail, Emmanouil Panaousis e Jens Grossklags (2018), "An Options Approach to Cybersecurity Investment", *IEEE Access*, 6, pp. 12175– 12186.
Disponível em: https://ieeexplore.ieee.org/document/8110826/ (consultado em 19 de abril 2018)
CIONET (2015), *Special Interest Group on Security - Key findings and conclusions*.
Disponível em: https://www.cionet.com/Data/files/groups/SIGreport_web.pdf
Cisco (2017), *Cisco 2017 Annual Cybersecurity Report*.
Disponível em: https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017 (consultado em 26 de junho 2017).
CNPD (2018), *Parecer n.º 14/2018, sobre a Proposta de Lei n.º119/XIII, que estabelece o regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148*.
Disponível em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=4236 (consultado em 19 de abril 2018).
Coelho, José Dias, António Simões Monteiro, Francisco Tomé, Henrique Mamede, José Gomes Almeida, Luís Pinto e Luís Vidigal (2012) (orgs.), *Repensar a Sociedade da Informação e do Conhecimento no Inicio do Século XXI*, Lisboa, Edições Sílabo.
Comissão Europeia (2009), *COM(2009) 149 final – Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões relativa à protecção das infra-estruturas críticas da informação, "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"*, Bruxelas.
Comissão Europeia (2012), *COM(2012) 140 final – Comunicação da Comissão ao Conselho e ao Parlamento Europeu, Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade*, Bruxelas.
Comissão Europeia (2013), *JOIN(2013) 1 final – Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*, Bruxelas.
Comissão Europeia (2015), *COM(2015) 192 final – Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, Estratégia para o Mercado Único Digital na Europa*, Bruxelas.
Comissão Europeia (2016), *COM(2016) 180 final – Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, Digitalização da Indústria Europeia – Usufruir de todos os benefícios do Mercado Único Digital*, Bruxelas.
Comissão Europeia (2016a), *Compreender as políticas da União Europeia: Um mercado único digital para a Europa*, Luxemburgo, Serviço das Publicações da União Europeia.
Comissão Europeia (2017), *JOIN(2017) 450 final – Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*, Bruxelas.
Comissão Europeia (2017a), *Cybersecurity in the European Digital Single Market – High Level Group of Scientific Advisors, Scientific Opinion 02*, Bruxelas.
Comissão Europeia (2017b), *COM(2017) 477 final – Proposta de "Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)"*, Bruxelas.

Comissão Europeia (2018), *COM(2018) 434 final – Proposta de "Regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027"*, Bruxelas.

COMPETE 2020 (2015), *Programa Operacional Competitividade e Internacionalização (COMPETE 2020) - Sobre nós*.

Disponível em: http://www.poci-compete2020.pt/sobre-nos (consultado em 22 de outubro 2017).

COMPETE 2020 (2015a), *Programa Operacional Competitividade e Internacionalização (COMPETE 2020) – Estrutura e Objectivos*.

Disponível em: http://www.poci-compete2020.pt/sobre-nos/estrutura-objectivos-programa (consultado em 22 de outubro 2017).

COMPETE 2020 (2017), *Ponto de Situação dos Sistemas de Incentivos às Empresas do Portugal 2020*, edição n.º 29 de 07 de dezembro de 2017.

Disponível em: http://www.poci-compete2020.pt/admin/fileman/Uploads/PS/20171221_PS_Incentivos_30NOV17.pdf (consultado em 24 de dezembro 2017).

Correia, Pedro Miguel Alves Ribeiro, Susana Isabel da Silva Santos e João Abreu de Faria Bilhim (2016), "Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio", *Revista da FAE*, 19 (2), pp. 22–37.

Disponível em: https://revistafae.fae.edu/revistafae/article/view/98 (consultado em 19 de maio 2018).

Correia, Pedro Miguel Alves Ribeiro, Susana Isabel da Silva Santos e João Abreu de Faria Bilhim (2017), "Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime", *Sociologia*, 33, pp. 95–113.

Disponível em: http://www.scielo.mec.pt/pdf/soc/v33/v33a06.pdf (consultado em 19 de maio 2018).

Craigen, Dan, Nadia Diakun-Thibault e Randy Purse (2014), "Defining Cybersecurity", *Technology Innovation Management Review*, October, pp. 13–21.

Disponível em: https://www.researchgate.net/publication/267631801_Defining_Cybersecurity (consultado em 27 de abril 2018).

Daniels, Susan (2017), "Protecting Against Cyber Risks "Beasts" come in all shapes and sizes", *Claims Magazine*, 65 (10), pp. 41-43.

Department for Culture Media & Sport (2017), *Cyber security breaches survey 2017*, London, Crown.

Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (consultado em 19 de abril 2018)

Department for Culture Media & Sport (2018), *Cyber security breaches survey 2018*, London, Crown.

Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (consultado em 09 de junho 2018)

DeSmit, Zach, Ahmad E. Elhabashya, Lee J. Wells e Jaime A. Camelio (2016), "Cyber-physical Vulnerability Assessment in Manufacturing Systems", *Procedia Manufacturing*, 5, pp. 1060–1074.

Disponível em: https://www.sciencedirect.com/science/article/pii/S2351978916300877 (consultado em 18 de abril 2018)

Dietzel, Bob (2018), “Playing it Safe: Cyber Security for Small- to Medium-Sized Businesses”, *Claims Magazine*, January, 66 (1), pp. 16-17.

Disponível em: http://web1.beta.propertycasualty360.com/2018/01/25/playing-it-safe-cybersecurity-for-small--to-medium?t=education-training (consultado em 18 de abril 2018).

Donohue, Laura K. (2016), *The Future of Foreing Intelligence – Privacy and Surveillance in a Digital Age*, New York, Oxford University Press.

Downes, Larry e Paul Nunes (2013), "Big-bang disruption: a new kind of innovator can wipe out incumbents in a flash ", *Harvard Business Review*, 91, 3 March/April, pp. 44–56.

Disponível em: https://hbr.org/2013/03/big-bang-disruption (consultado em 19 de fevereiro 2018).

Drucker, Peter (2015), *Sociedade Pós-Capitalista*, Coimbra, Conjuntura Actual Editora. (1.ª edição 2003)

Earley, Seth (2014), "The Digital Transformation: Staying Competitive", *IT Professional*, 16, 2 March/April, pp. 58–60.

Disponível em: https://doi.org/10.1109/MITP.2014.24 (consultado em 16 de janeiro 2018).

ECO e Isabel Patrício (2018), “Startup portuguesa fecha. Não é capaz de cumprir RGPD”, *Economia Online* (online), 24 de maio.

Disponível em: https://eco.pt/2018/05/24/startup-portuguesa-fecha-nao-e-capaz-de-cumprir-rgpd/ (consultado em 24 de maio 2018).

EY (2016), *Path to cyber resilience: Sense, resist, react – EY’s 19th Global Information Security Survey 2016-17*.

Disponível em: http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016 (consultado em 26 de outubro 2016).

ENISA (2012), *Cyber Incident Reporting in the EU: An overview of security articles in EU legislation*, Agosto, Heraklion.

ENISA (2014), *Roadmap for NIS education programmes in Europe,* October, Heraklion.

Disponível em: https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe/at_download/fullReport.

ENISA (2017), “ENISA Threat Landscape Report 2016 – 15 Top Cyber-Threats and Trends”*, OPSEC*, janeiro, Heraklion.

ENISA (2017a), *Cyber Security Culture in organisations,* November, Heraklion.

Disponível em: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

ENISA (2018), *Looking into the crystal ball*, versão 1.0, January, Heraklion.

Disponível em: https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball.

ENISA (2018a), “ENISA Threat Landscape Report 2017 – 15 Top Cyber-Threats and Trends”*, OPSEC*, janeiro, Heraklion.

EPRS (2015), “Industry 4.0: Digitalisation for productivity and growth”, *Briefing*, (Online), September.

Disponível em: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282015%29568337

Etzioni, Amitai (2011), “Cybersecurity in the Private Sector”, *Issues in Science and Technology*, 28 (1), pp. 58–62.

Disponível em: http://web1.beta.propertycasualty360.com/2018/01/25/playing-it-safe-cybersecurity-for-small--to-medium?t=education-training (consultado em 18 de abril 2018).

Europol (2018), *Internet Organised Crime Threat Assessment 2018*, Haia, European Union Agency for Law Enforcement Cooperation.

Disponível em: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

Eurostat (2013), *Science, technology and innovation in Europe*, Luxembourg, Publications Office of the European Union.

Disponível em: http://ec.europa.eu/eurostat/documents/3930297/5969406/KS-GN-13-001-EN.PDF

Evangelista, Rinaldo, Paolo Guerrieri e Valentina Meliciani (2014), "The economic impact of digital technologies in Europe", *Economics of Innovation and New Technology*, 23:8, pp. 802–824.

Disponível em: http://dx.doi.org/10.1080/10438599.2014.918438, disponível em: https://www.researchgate.net/publication/266400553_The_economic_impact_of_digital_technologies_in_Europe .

FERMA (2017), *At the junction of corporate governance & cybersecurity*, Brussels.

Disponível em: https://www.ferma.eu/sites/default/files/inline-files/WEB-FERMA-Brochure2017%2029%20June_0_0.pdf

Fernandes, Nuno Serra (2018), "Só 8% das empresas estão preparadas para as novas regras de Proteção de Dados", *TSF Rádio Notícias* (online), 23 de maio.

Disponível em: https://www.tsf.pt/sociedade/interior/so-8-das-empresas-estao-preparadas-para-as-novas-regras-de-protecao-de-dados-9368476.html (consultado em 24 de maio 2018).

Ferrão, João (2015), "Ambiente e território: para uma nova geração de políticas públicas com futuro", *Afirmar o futuro: políticas públicas para Portugal*, 2, pp. 328-336. Lisboa, Fundação Calouste Gulbenkian.

Disponível em: http://hdl.handle.net/10451/19991 (consultado em 16 de março 2018).

Ferreira, J. M. Carvalho, José Neves e António Caetano (2001) (coords), *Manual de psicossociologia das organizações*, Lisboa, McGraw-Hill.

Ferreira, Luís Miguel (2015), *A Sociedade da Informação nas regiões portuguesas: medir para desenvolver*, Lisboa, Chiado Editora.

Franklin, Daniel (2017) (coord.), *Megatech: As grandes inovações do futuro*, Lisboa, Clube do Autor.

Gibson, Kevin (2000), "The Moral Basis of Stakeholder Theory", *Journal of Business Ethics*, 26 (3), pp. 245-257.

Glenny, Misha (2011), *Dark Market: cyberthieves, cybercops and you*, London, The Bodley Head.

Glorioso, Ludovica (2015), *National Cyber Security Organisation: Italy*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

GNS (2018), "RGPD e a Segurança das Redes e Sistemas de Informação, Manual de Boas Práticas – Parte I: Deveres e responsabilidades das organizações".

Disponível em: https://www.gns.gov.pt/media/10691/MBP%20I_Deveres%20e%20Responsabilidades_V1_16ABR18.pdf (consultado em 25 de maio 2018).

GNS (2018a), "RGPD e a Segurança das Redes e Sistemas de Informação, Manual de Boas Práticas – Parte II: Contributos para políticas e procedimentos".

Disponível em: https://www.gns.gov.pt/media/10694/MBP%20II_Contributos%20para%20Pol%C3%ADticas%20e%20Procedimentos_V1_16ABR18.pdf (consultado em 25 de maio 2018).

GNS (2018b), "RGPD e a Segurança das Redes e Sistemas de Informação, Manual de Boas Práticas – Parte III: Segurança Física".

Disponível em: https://www.gns.gov.pt/media/10697/MBP%20III_Seguran%C3%A7a%20F%C3%ADsica_V1_16ABR18.pdf (consultado em 25 de maio 2018).

Godinho, Manuel Mira e Ricardo Paes Mamede (2016), "Southern Europe in crisis: industrial policy lessons from Italy and Portugal", *Economia e Politica Industriale*, 43, pp. 331-336.

Disponível em: https://doi.org/10.1007/s40812-016-0037-6

Gordon, Lawrence A. e Martin P. Loeb (2002), "The economics of information security investment", *ACM Transactions on Information and System Security (TISSEC)*, 5 (4), November, pp. 438–457.

Disponível em: https://dl.acm.org/citation.cfm?id=581274 (consultado em 3 de junho 2018)

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn e Lei Zhou (2015), "The impact of information sharing on cybersecurity underinvestment: A real options perspective", *Journal of Accounting and Public Policy*, 34 (5), pp. 509–519.

Disponível em: https://www.sciencedirect.com/science/article/pii/S0278425415000423 (consultado em 19 de abril 2018)

Gordon, Lawrence A., Martin P. Loeb e Lei Zhou (2016), "Investing in Cybersecurity: Insights from the Gordon-Loeb Model", *Journal of Information Security*, 7 (2), March, pp. 49–59.

Disponível em: http://www.scirp.org/journal/PaperInformation.aspx?paperID=64892 (consultado em 19 de abril 2018)

Gouveia, Jorge Bacelar e Sofia Santos (coord.) (2015), *Enciclopédia de Direito e Segurança*, Coimbra, Almedina.

Gouveia, Luis Borges e Raul Carvalho Morgado (2017), "Estratégia Nacional de Segurança do Ciberespaço", *Relatório Interno TRS 10/2017*, Working Paper.

Disponível em: https://bdigital.ufp.pt/handle/10284/6032 (consultado em 09 de novembro 2017).

Gray, Jeff e Bernhard Rumpe (2017), "Models for the digital transformation", *Software & Systems Modeling*, 16, pp. 307–308.

Disponível em: https://doi.org/10.1007/s10270-017-0596-7

Hackett, Robert (2015), "What to know about the Ashley Madison hack", *Fortune* (online), 26 de Agosto.

Disponível em: http://fortune.com/2015/08/26/ashley-madison-hack/ (consultado em 28 de agosto 2015).

Harvard Business Review (2014), "The Digital Transformation of Business", *Harvard Business Review* (online), 01 de setembro.

Disponível em: https://hbr.org/sponsored/2014/09/the-digital-transformation-of-business (https://hbr.org/resources/pdfs/comm/microsoft/the_digital_transformation_of_business.pdf consultado em 12 de janeiro 2018).

Heinrich, Stefan (2014), "Socio-economic consequences of digital transformation", *Socioeconomica*, 3 (6), pp. 179–202.

Disponível em: http://www.socioeconomica.info/xmlui/bitstream/handle/11171/142/1%20Stefan%20Heinrich.pdf

Hern, Alex e Samuel Gibbs (2015), "Ashley Madison hackers release vast database of 33m accounts", *The Guardian* (online), 19 de Agosto.

Disponível em: https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts (consultado em 19 de agosto 2015).

Hess, Thomas, Christian Matt, Alexande Benlian e Florian Wiesböck (2016), "Options for Formulating a Digital Transformation Strategy", *MIS Quarterly Executiv,* 15, pp 103-119.

Disponível em: https://www.researchgate.net/publication/291349362_Options_for_Formulating_a_Digital_Transformation_Strategy

Hidalgo, César (2015), *Why Information Grows*, London, Penguin Books.

HM Treasury (2011), *The Magenta Book: Guidance for evaluation*, London, Crown.

Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/220542/magenta_book_combined.pdf.

Hriciková, Lea e Kadri Kaska (2015), *National Cyber Security Organisation: Slovakia*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Hutchins, Margot J., Raunak Bhinge, Maxwell K. Micali, Stefanie L. Robinson, John W. Sutherland e David Dornfeld (2015), "Framework for Identifying Cybersecurity Risks in Manufacturing", *Procedia Manufacturing*, 1, pp. 47–63.

Disponível em: https://www.sciencedirect.com/science/article/pii/S2351978915010604 (consultado em 18 de abril 2018)

IAPMEI (2017), *Guia de Informação Indústria 4.0 Sistemas de Incentivos à Economia Digital*, 1.ª edição de outubro de 2017.

Disponível em: https://www.iapmei.pt/getattachment/Paginas/Industria-4-0/GuiaIndustria40.pdf.aspx (consultado em 24 de dezembro 2017).

IAPMEI (2018), "Regime Geral de Proteção de Dados – Relatório do Inquérito de Avaliação da Maturidade das PME's face ao RGPD – 2018".

Disponível em: https://www.iapmei.pt/getattachment/PRODUTOS-E-SERVICOS/Assistencia-Tecnica-e-Formacao/Regime-Geral-de-Protecao-de-Dados/RGPD-Inquerito-PME-2018.pdf.aspx?lang=pt-PT (consultado em 1 de julho 2018).

IDN-CESEDEN (2013), "Estratégia da Informação e Segurança no Ciberespaço", *IDN Cadernos 12*, Instituto da Defesa Nacional.

Disponível em: https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

INE (2017), *Destaque Informação à Comunicação Social sobre o Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas 2017*, de 21 de novembro de 2017.

Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=281440228&DESTAQUEStema=55483&DESTAQUESmodo=2 (consultado em 24 de dezembro 2017).

INE (2017a), *Anuário Estatístico de Portugal 2016*, Lisboa, Instituto Nacional de Estatística, I.P.

Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=277187869&PUBLICACOESmodo=2 (consultado em 13 de fevereiro 2018).

INE (2018), *Empresas em Portugal 2016*, fevereiro, Lisboa, Instituto Nacional de Estatística, I.P.

Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=318224733&PUBLICACOESmodo=2 (consultado em 13 de fevereiro 2018).

Internet Society (2012), *Some Perspectives on Cybersecurity 2012.*

Disponível em: https://www.internetsociety.org/resources/doc/2012/some-perspectives-on-cybersecurity-2012/ (https://cdn.prod.internetsociety.org/wp-content/uploads/2017/08/bp-deconstructing-cybersecurity-16nov-update.pdf) (consultado em 03 de dezembro 2016).

Isaías, Pedro, Ivo Dias de Sousa, Luísa Cagica Carvalho, Bráulio Alturas (2017), *E-Business e Economia Digital*, Lisboa, Edições Sílabo.

ITI (2011), *The IT Industry's Cybersecurity Principles for Industry and Government*, Washington, Information Technology Industry Council (ITI).

Disponível em: http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf (consultado em 22 de novembro 2017).

Jorgenson, Dale W. e Kuong M. Vu (2016), "The ICT revolution, world economic growth, and policy issues", *Telecommunications Policy*, 40, pp. 383–397.

Disponível em: http://dx.doi.org/10.1016/j.telpol.2016.01.002

JOUE (2003), *Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas C(2003) 1422*, Bruxelas.

JOUE (2016), *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*, Bruxelas.

JOUE (2016a), *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*, Bruxelas.

Kaska, Kadri (2015), *National Cyber Security Organisation: the Netherlands*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Kattel, Rainer e Mariana Mazzucato (2018), "Mission-oriented innovation policy and dynamic capabilities in the public sector", *Working Paper Series (IIPP WP 2018-5)*, London, UCL Institute for Innovation and Public Purpose.

Disponível em: http://www.ucl.ac.uk/bartlett/public-purpose/wp2018-05 (consultado em 31 de julho 2018).

Khan, Shahyan (2016), *Leadership in the digital age – A study on the effects of digitalisation on top management leadership*, Dissertação de Mestrado, Estocolmo, Stockholm University – Stockholm Business School.

Disponível em: http://su.diva-portal.org/smash/get/diva2:971518/FULLTEXT02.pdf

Kim, Won, Ok-Ran, Jeong Chulyun Kim e Jungmin So (2010), "The dark side of the Internet: Attacks, costs and responses", *Information Systems*, 36, pp. 675–705.

Disponível em: https://doi.org/10.1016/j.is.2010.11.003

Kovács, László e Gergely Szentgáli (2015), *National Cyber Security Organisation: Hungary*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

KPMG (2017), "O Impacto do Regulamento Geral de Protecção de Dados em Portugal".

Disponível em: https://home.kpmg.com/pt/pt/home/insights/2017/10/impact-of-gdpr.html [https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf] (consultado em 2 de julho 2017).

KPMG (2018), *Risco e Resiliência – Estudo da Continuidade do Negócio em Portugal*, fevereiro, KPMG Advisory – Consultores de Gestão, S.A.

Disponível em: https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2018-business-continuity-risk-resilience.pdf.

Kriz, Danielle (2011), "Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity", *2011 Second Worldwide Cybersecurity Summit (WCS)*, London, pp. 1-3.

Disponível em: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978798&isnumber=5978775 (consultado em 22 de novembro 2017).

Lam, Wing Man Wynne (2016), "Attack-prevention and damage-control investments in cybersecurity", *Information Economics and Policy*, 37, pp.42–51.

Disponível em: https://www.sciencedirect.com/science/article/pii/S0167624516301263 (consultado em 19 de abril 2018)

Lampreia, J. Martins e Daniel Guéguen (2008), *O Lóbi na União Europeia*, Lisboa, Texto Editora.

Landau, Susan (2013)*, Surveillance or Security? The Risk Posed by New Wiretapping Technologies*, London, The MIT Press.

Lember, Veiko, Rainer Kattel e Piret Tõnurist (2018), "Technological Capacity in the Public Sector: The Case of Estonia", *Working Paper Series (IIPP WP 2017-03)*, London, UCL Institute for Innovation and Public Purpose.

Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2018/jan/technological-capacity-public-sector-case-estonia (consultado em 24 de novembro 2017).

Lopes, Mónica (2013), "A avaliação de políticas públicas em Portugal: marcos de um desenvolvimento incipiente", comunicação apresentada no *IV Colóquio Internacional de Doutorandos/as do CES "Coimbra C: Dialogar com os Tempos e os Lugares do(s) Mundo(s)"*, 6 – 7 de dezembro 2013, Coimbra.

Disponível em: http://hdl.handle.net/10316/41173 (consultado em 16 de março 2018)

Lopes, Raul (2001)*, Competitividade, Inovação e Territórios*, Oeiras, Celta Editora.

Lusa (2018), "Ministro reitera ambição de liderar área do digital", *Açoriano Oriental*, 11 de abril, p. 19.

Lusa (2018a), "Ex-coordenador de cibersegurança ataca "falta de coragem" do governo para reformar setor", *Diário de Notícias* (online), 12 de junho.

Disponível em: https://www.dn.pt/lusa/interior/ex-coordenador-de-ciberseguranca-ataca-falta-de-coragem-do-governo-para-reformar-setor-9439795.html (consultado em 12 de junho 2018).

Mações, Manuel (2017), *Planeamento, Estratégia e Tomada de Decisão*, Lisboa, Conjuntura Actual Editora.

MadreMedia/Lusa (2018), "Costa quer acelerar 'cluster' da cibersegurança em Portugal", *Sapo24* (online), 12 de junho.

Disponível em: https://24.sapo.pt/atualidade/artigos/costa-quer-acelerar-cluster-da-ciberseguranca-em-portugal (consultado em 12 de junho 2018).

Mayer-Schönberger, Viktor (2011), *Delete: the virtue of forgetting in digital age*, New Jersey, Princeton University Press.

Mamede, Ricardo Paes e Paulo Areosa Feio (2012), *Institutional conditions for effective and legitimate industrial policies: the case of Portugal*, Working Paper, Lisboa, DINÂMIA'CET - ISCTE-IUL.

Disponível em: http://hdl.handle.net/10071/5142 (consultado em, 21 de novembro 2017).

Marcelino, Valentina (2018), "Mesmo em coisas mais simples as restrições orçamentais foram uma dificuldade", *Diário de Notícias* (online), 12 de junho.

Disponível em: https://www.dn.pt/portugal/interior/ciberseguranca-mesmo-em-coisas-mais-simples-as-restricoes-orcamentais-foram-uma-dificuldade-9430873.html (consultado em 12 de junho 2018).

Marques, A. H. de Oliveira (1998), *História de Portugal – Volume III – Das revoluções liberais aos nossos dias*, Lisboa, Editorial Presença.

MARSH (2016), *Continental European Cyber Risk Survey: 2016 Report*.

Disponível em: https://www.marsh.com/cy/en/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html (consultado em 02 de novembro 2016).

MARSH (2017), *A Visão das Empresas Portuguesas sobre os Riscos 2017*.

Disponível em: https://static.computerworld.com.pt/media/2017/03/A-Visao-das-Empresas-Portuguesas-sobre-os-Riscos-2017.pdf (consultado em 25 de abril 2018).

MARSH (2018), *A Visão das Empresas Portuguesas sobre os Riscos 2018*.

Disponível em: https://static.computerworld.com.pt/media/2018/04/Estudo-Marsh-A-Visao-das-Empresas-Portuguesas-sobre-os-Riscos-2018.pdf (consultado em 25 de abril 2018).

Mathews, Dan (2016), "What makes criminal hackers want to hack?", *Racounter* (online), 27 de novembro.

Disponível em: https://www.raconteur.net/risk-management/why-smes-are-big-targets-for-cyber-crime (consultado em 16 de setembro 2018).

Matos, Pedro Carvalhais de Abreu (2015), *A participação dos stakeholders em processos de decisão da União Europeia – o caso da Estratégia da União Europeia para a cibersegurança*, Dissertação de Mestrado em Ciência Política e Relações Internacionais, Lisboa, FCSH-UNL.

Matt, Christian, Thomas Hess e Alexander Benlian (2015), "Digital Transformation Strategies", *Business and In-formation Systems Engineering*, 57(5), pp. 339–343.

Disponível em: https://link.springer.com/content/pdf/10.1007/s12599-015-0401-5.pdf

Mayadunne, Sanjaya e Sungjune Park (2016), "An economic model to evaluate information security investment of risktaking small and medium enterprises", *Int. J. Production Economics*, 182, December, pp. 519–530.

Disponível em: https://www.sciencedirect.com/science/article/pii/S092552731630250X (consultado em 19 de abril 2018)

Mazzucato, Mariana (2014), *The Entrepreneurial State*, London, Anthem Press.

Mazzucato, Mariana (2018), *The Value of Everything – Making and Taking in the Global Economy*, London, Alan Lane.

Meffet, Jürgen e Pedro Mendonça (2017), *Digital@Scale*, Lisboa, Planeta Manuscrito.

Minárk, Tomáš (2016), *National Cyber Security Organisation: Czech Republic*, 2nd revised edition,Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Monteiro, Mafalda Simões (2018), "A cibersegurança tem de ter um racional de negócio", *Computerworld* (online), 21 de fevereiro.
Disponível em: https://www.computerworld.com.pt/2018/02/21/a-ciberseguranca-tem-de-ter-um-racional-de-negocio/ (consultado em 31 de agosto 2018).

Moore, Tyler (2010), "The economics of cybersecurity: Principles and policy options", *International Journal of Critical Infrastructure Protection*, 3, pp.103–117.

MSI – Missão para a Sociedade da Informação (1997), *Livro Verde para a Sociedade da Informação em Portugal*, Lisboa, Ministério da Ciência e da Tecnologia.

Mukhopadhyay, Arunabha, Samir Chatterjee, Debashis Saha, Ambuj Mahanti e Samir K. Sadhukhan (2013), "Cyber-risk decision models: To insure IT or not?", *Decision Support Systems*, 56, December, pp.11–26.
Disponível em: https://www.sciencedirect.com/science/article/pii/S0167923613001115 (consultado em 23 de novembro 2017)

Müller, Egon e Hendrik Hopf (2017), "Competence Center for the Digital Transformation in Small and Medium-Sized Enterprises", *Procedia Manufacturing*, 11, pp. 1495–1500.
Disponível em: https://www.sciencedirect.com/science/article/pii/S2351978917304894 (consultado em 16 de janeiro 2018)

Murgeira, Raquel (2018), "Cibersegurança preocupa mais de 90% das empresas portuguesas", *Jornal de Negócios* (online), 6 de março.
Disponível em: https://www.jornaldenegocios.pt/empresas/detalhe/ciberseguranca-preocupa-mais-de-90-das-empresas-portuguesas (consultado em 21 de maio 2018).

Nakamura, Leonard, Jon Samuels e Rachel Soloveichik (2017), "Measuring the "Free" Digital Economy within the GDP and Productivity Accounts", *FRB of Philadelphia Working Paper No. 17-37*.
Disponível em: https://ssrn.com/abstract=3058017

Nelson, Richard R. (2017), "Thinking About Technology Policy: 'Market Failures' versus 'Innovation systems'", *Working Paper Series (IIPP WP 2017-02)*, London, UCL Institute for Innovation and Public Purpose.
Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2018/jan/thinking-about-technology-policy-market-failures-versus-innovation-systems (consultado em 2 de abril 2018).

Klimburg, Alexander (2012), *National Cyber Security Framework Manual*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Nagurney, Anna e Shivani Shukla (2017), "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability", *European Journal of Operational Research*, 260 (2), July, pp. 588–600.
Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0377221716310682 (consultado em 19 de abril 2018)

NCI (2017), "NATO breaks ground on Portugal IT Academy", *NATO Communications and Information Agency* (online), 23 de maio.
Disponível em: https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx (consultado em 25 de maio 2017).

Newcomer, Eric (2017), "Uber Paid Hackers to Delete Stolen Data on 57 Million People", *Bloomberg* (online), 21 de novembro.

Disponível em: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (consultado em 21 de novembro 2017).

Nextvalue e CIONET (2016), *Digital Transformation in Europe: What's Next*.

Disponível em: http://www.cionet.com/Data/files/groups/Report%20Digital%20Transformation%20in%20EU.pdf

Nóbrega, João (2017), "Tribolet desafia empresas a viabilizarem curso de cibersegurança", *Computerworld* (online), 08 de fevereiro.

Disponível em: https://www.computerworld.com.pt/2017/02/08/tribolet-desafia-empresas-a-viabilizarem-curso-de-ciberseguranca/ (consultado em 07 de junho 2018).

Nunes, Paulo Viegas (2015), *Sociedade em Rede, Ciberespaço e Guerra de Informação*, Lisboa, Instituto da Defesa Nacional.

Nunes, Paulo Viegas, (2016), "Ciberameaças e quadro legal dos conflitos no ciberespaço", em João Vieira Borges e Teresa Ferreira Rodrigues (coord.), *Ameaças e Riscos Transnacionais no novo Mundo Global*, Porto, Fronteira do Caos.

Nunes, Paulo Viegas (2018) (coord.), "Contributos para uma Estratégia Nacional de Ciberdefesa", *IDN Cadernos 28*, Instituto da Defesa Nacional.

Disponível em: https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

Nye, Jr., Joseph S. (2012), *O Futuro do Poder*, Lisboa, Círculo dos Leitores.

Obercom (2016), "Políticas Públicas para a Sociedade de Informação e Media", *Relatórios Obercom*, (online), Setembro.

Disponível em: https://obercom.pt/politicas-publicas-para-sociedade-de-informacao-e-media/

Observatório do QREN (2009), *Concepção Geral do Processo de Monitorização Estratégica do QREN*, e+ cadernos do Observatório do QREN.

Disponível em: http://www.adcoesao.pt/sites/default/files/desenvolvimento_regional/zooms_territoriais/ecadernoqren_6.pdf (consultado em 26 de junho 2018).

OCDE (1996), *The Knowledge-Based Economy*, Paris, OECD Publishing.

Disponível em: https://www.oecd.org/sti/sci-tech/1913021.pdf

OCDE (2001), *Measurement of Aggregate and Industry-level Productivity Growth*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264194519-en

OCDE (2008), *OECD Council Recommendation on the Protection of Critical Information Infrastructures*, Paris, OECD Publishing.

Disponivel em https://www.oecd.org/sti/40825404.pdf

OCDE (2010), *OECD Information Technology Outlook 2010*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/it_outlook-2010-en

OCDE (2012), *OECD Internet Economy Outlook 2012*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264086463-en

OCDE (2012a), *Cybersecurity Policy Making at a Turning Point*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/5k8zq92vdgtl-en

OCDE (2014), *Measuring the Digital Economy: A New Perspective*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264221796-en

OCDE (2015), *OECD Digital Economy Outlook 2015*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264232440-en

OCDE (2015a), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264245471-en

OCDE (2017), *OECD Digital Economy Outlook 2017*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264276284-en

OCDE (2017a), *The Next Production Revolution: Implications for Governments and Business*, Paris, OECD Publishing.

Disponível em: http://dx.doi.org/10.1787/9789264271036-en

OCDE (2017b), *Going Digital: Making the Transformation Work for Growth and Well-Being*, Meeting of the OECD Council at Ministerial Level, Paris, OECD Publishing.

Disponível em: https://www.oecd.org/mcm/documents/C-MIN-2017-4%20EN.pdf

ONU (2003), *Resolution adopted by the General Assembly 57/239. Creation of a global culture of cybersecurity – A/RES/57/239*, 31 de janeiro.

Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

Osula, Anna-Maria (2015), *National Cyber Security Organisation: United Kingdom*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Osula, Anna-Maria (2015a), *National Cyber Security Organisation: Estonia*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Paul, Sneha (2017), "Reinforcing your SME against cyberthreats", *Computer Fraud & Security*, 2017 (10), October, pp. 13–15 (consultado via b-on.pt em 18 de abril 2018)

Paulsen, Celia (2016), "Cybersecuring Smal Businesses", *Computer*, 49 (8), pp.92-97.

Disponível em: http://dx.doi.org/10.1109/MC.2016.223.

Paulsen, Celia e Patricia Toth (2016a), *Small Business Information Security: The Fundamentals - NISTIR 7621, Revision 1*, Gaithersburg, NIST - National Institute of Standards and Technology, U.S. Department of Commerce.

Disponível em: https://doi.org/10.6028/NIST.IR.7621r1.

Pawlak, Patryk e Cécile Wendling (2013), "Trends in cyberspace: can governments keep up?", *Environment Systems and Decisions*, December, 33 (4), pp. 536–543.

Disponível em: https://link.springer.com/article/10.1007%2Fs10669-013-9470-5 (consultado em 24 de outubro 2017).

Pequenino, Karla (2018), "Cibersegurança: Profissionais, procuram-se", *Público*, 1 de junho, pp. 28-29.

Pereira, Teresa e Henrique Santos (2014), "Challenges in Information Security Protection", comunicação apresentada na *13th European Conference on Cyber Warfare and Security (ECCWS-2014)*, Piraeus, Greece.

Disponível em: https://www.researchgate.net/publication/264116803_Challenges_in_Information_Security_Protection (consultado em 16 de novembro 2017).

Pernik, Piret, Jesse Wojtkowiak e Alexander Verschoor-Kirss (2016), *National Cyber Security Organisation: United States*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.

Petit, François e Michel Dubois (1998), *Introdução à psicossociologia das organizações*, Lisboa, Instituto Piaget.

Pintér, Róbert (2008) (ed.), *Information Society – From Theory to Political Practice*, Budapest, Gondolat – Új Mandátum.

Polanyi, Karl (2012), *A Grande Transformação – As Origens Políticas e Económicas do Nosso Tempo*, Lisboa, Edições 70.

Ponemon Institute (2018), *2018 Cost of Data Breach Study: Global Overview*, julho.
Disponível em: https://www.ibm.com/security/data-breach (consultado em 14 de agosto 2018).

Poppensieker, Thomas e Rolf Riemenschnitter (2018), *A new posture for cybersecurity in a networked world*, setembro.
Disponível em: https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world (consultado em 26 de setembro 2018).

Presidência do Conselho de Ministros (2010), *Resolução do Conselho de Ministros n.º 91/2010 - Diário da República n.º 225/2010, Série I de 2010-11-19, que aprova a Agenda Digital 2015, iniciativa inserida no âmbito do Plano Tecnológico*.
Disponível em: http://data.dre.pt/eli/resolconsmin/91/2010/11/19/p/dre/pt/html.

Presidência do Conselho de Ministros (2015), *Resolução de Conselho de Ministros n.º 22/2015 - Diário da República n.º 74/2015, Série I de 2015-04-16, que Procede à primeira alteração à Resolução do Conselho de Ministros n.º 112/2012, de 31 de dezembro, que aprovou a Agenda Portugal Digital.*
Disponível em: http://data.dre.pt/eli/resolconsmin/22/2015/04/16/p/dre/pt/html.

Presidência do Conselho de Ministros (2015a), *Resolução de Conselho de Ministros n.º 36/2015 - Diário da República n.º 113/2015, Série I de 2015-06-12, que aprova a Estratégia Nacional de Segurança do Ciberespaço.*
Disponível em: http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html.

Presidência do Conselho de Ministros (2017), *Resolução de Conselho de Ministros n.º 115/2017 - Diário da República n.º 163/2017, Série I de 2017-08-24, que cria o grupo de projeto denominado «Conselho Superior de Segurança do Ciberespaço»*.
Disponível em: http://data.dre.pt/eli/resolconsmin/115/2017/08/24/p/dre/pt/html.

Presidência do Conselho de Ministros (2018), *Despacho n.º 1195/2018 - Diário da República n.º 24/2018, Série II de 2018-02-02, que aprova o Regulamento Interno do Conselho Superior de Segurança do Ciberespaço*.
Disponível em: https://dre.pt/home/-/dre/114618044/details/maximized?serie=II&day=2018-02-02&date=2018-02-01&dreId=114618042.

Presidência do Conselho de Ministros (2018a), *Proposta de Lei n.º119/XIII, que estabelece o regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148*.
Disponível em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=4236 (consultado em 19 de abril e 7 de maio 2018).

Presidência do Conselho de Ministros (2018b), *Lei n.º 46/2018 - Diário da República n.º 155/2018, Série I de 2018-08-13, que Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*.
Disponível em: http://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html.

Quiggin, John (2014), "National accounting and the digital economy", *Economic Analysis and Policy*, 44, pp. 136–142.
Disponível em: http://dx.doi.org/10.1126/science.1130992
Reis, Rodolfo Alexandre (2018), "Parlamento chumba projeto para alteração na Comissão Nacional de Proteção de Dados", *O Jornal Económico* (online), 4 de maio.
Disponível em: http://www.jornaleconomico.sapo.pt/noticias/parlamento-chumba-projeto-para-alteracao-na-comissao-nacional-de-protecao-de-dados-302324 (consultado em 4 de maio 2018).
República Portuguesa (2018), "Novos investimentos em tecnologia e investigação criam empregos de qualidade em Portugal", *Portal do Governo* (online), 13 de junho.
Disponível em: https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=novos-investimentos-em-tecnologia-criam-empregos-de-qualidade-em-portugal (consultado em 14 de junho 2018).
Rettman, Andrew (2017), "EU agency to fight election hacking", *EUObserver* (online), 19 de setembro.
Disponível em: https://euobserver.com/justice/139072 (consultado em 20 de setembro 2017).
Rifkin, Jeremy (2016), *A Sociedade do Custo Marginal Zero*, Lisboa, Bertrand Editora.
Rosenquist, Matt (2015), *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*, Chicago, Caxton Business & Legal, Inc.
Ross, Alec (2016), *As Indústrias do Futuro*, Coimbra, Conjuntura Actual Editora.
Rotenberg, Marc, Julia Horwirtz e Jeramie Scott (2015), *Privacy in the Modern Age, the search for solutions*, New York, The New Press.
Rowe, Brent R. e Michael P. Gallaher (2006), "Private sector cyber security investment strategies: An empirical analysis", comunicação apresentada na *Conference: Workshop on the Economics of Information Security (WEIS)*, January.
Disponível em: https://www.researchgate.net/publication/228339552_Private_sector_cyber_security_investment_strategies_An_empirical_analysis (consultado em 13 de abril 2018)
RSA (2016), *Future Impacts: the changing nature of risk facing small businesses in the UK*, Reino Unido.
Disponível em: https://www.rsagroup.com/media/1911/rsa-future-impacts-research-findings-30-november-2016.pdf
Ruan, Keyun (2017), "Introducing cybernomics: A unifying economic framework for measuring cyber risk", *Computer & Security*, 65, pp.77-89.
Salavisa Lança, Isabel, Fátima Suleman e Maria de Fátima Guerreiro (2004) (orgs.*), Portugal e a Sociedade do Conhecimento*, Oeiras, Celta Editora.
Salavisa Lança, Isabel e Ana Cláudia Valente (2005) (coord.*), Inovação Tecnológica e Emprego – O caso Português*, Lisboa, Instituto para a Qualidade na Formação, I.P..
Santos, Lino (2011), *Contributos para uma melhor governação da cibersegurança em Portugal*, Dissertação de Mestrado em Direito e Segurança, Lisboa, FD-UNL.
Santos, Lino e Armando Marques Guedes (2015), "Breves reflexões sobre Poder e Ciberespaço", *RDeS – Revista de Direito e Segurança*, 6, pp. 189-209.
Disponível em: https://comum.rcaap.pt/bitstream/10400.26/14329/1/PodereCiberesa%C3%A7o.pdf
Shackelford, Scott J. (2012), "Should your firm invest in cyber risk insurance?", *Business Horizons*, 55 (4), July-August, pp. 349–356.

Disponível em: https://www.sciencedirect.com/science/article/pii/S0007681312000377 (consultado em 18 de abril 2018)

Schatz, Daniel, Rabih Bashroush e Julie Wall (2017) "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law*, 12 (2) Article 8, pp 53-74.

Disponível em: https://commons.erau.edu/jdfsl/vol12/iss2/8

Schmidt, Eric e Jared Cohen (2013), *The New Digital Age: reshaping the future of people, nations and business*, London, John Murray.

Schneier, Bruce (2015), *Data and Goliath*, New York, W. W. Norton.

Schwab, Klaus (2017), *The Global Competitiveness Report 2017–2018*, Geneva, World Economic Forum.

Disponível em: http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017%E2%80%932018.pdf

Schwab, Klaus (2017a), *A Quarta Revolução Industrial*, Oeiras, Levoir.

Sistema de Segurança Interna (2018), *Relatório Anual de Segurança Interna 2017*.

Disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6 (consultado em 30 de março 2018).

Sommer, Peter e Ian Brown (2011), "Reducing Systemic Cybersecurity Risk", *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3*, Paris.

Disponível em: https://www.oecd.org/gov/risk/46889922.pdf

Sousa, António Freitas de (2018), "Empresas portuguesas com forte apetência pelo digital", *O Jornal Económico*, 7 de julho, p. 26.

Stanton, Mandy, George Ernst e Anton L. Janik, Jr. (2017), "Cybersecurity Best Practices", *The Computer & Internet Lawyer*, 34 (4), April, pp. 22–25 (consultado via b-on.pt em 8 de novembro 2017)

Stark, John Reed (2017), "Top Cybersecurity Concerns for Every Director", *Corporate Governance Advisor*, 25 (2), March/April pp. 1–9.

Disponível em: https://www.johnreedstark.com/wp-content/uploads/sites/180/2017/02/April-17.pdf (consultado em 8 de novembro 2017)

Symantec (2016), *Attackers Target Both Large and Small Businesses* (infografia).

Disponível em: https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf (consultado em 16 de setembro 2018)

Symantec (2017), *Internet Security Threat Report*, 22, EUA.

Disponível em: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec (2018), *Internet Security Threat Report*, 23, EUA.

Disponível em: https://www.symantec.com/security-center/threat-report

Teodoro, Nuno, Luis Gonçalves e Carlos Serrão (2015), "NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements", *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, pp. 418-425.

Disponível em: https://ieeexplore.ieee.org/document/7345310/ (consultado em 16 de maio 2018).

Terceiro, José B. (1997), *Socied@de Digit@l – do homo sapiens ao homo digitalis*, Lisboa, Relógio D'Água Editores.

The White House (2015), "FACT SHEET: President Xi Jinping's State Visit to the United States", *Office of the Press Secretary*, September 25, Washington DC.

Disponível em: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (consultado em 7 de junho 2017).

Toesland, Finbarr (2016), "Why SMEs are big targets for cyber crime", *Racounter* (online), 27 de novembro.

Disponível em:https://www.raconteur.net/risk-management/why-smes-are-big-targets-for-cyber-crime (consultado em 16 de setembro 2018).

Toffler, Alvin (1991), *Os Novos Poderes*, Lisboa, Livros do Brasil.

Thomas, Kurt, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, Daniel Margolis, Vern Paxson e Elie Bursztein (2017), "Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials", comunicação apresentada na *2017 ACM SIGSAC Conference on Computer and Communications Security*, 30 outubro – 3 de novembro 2017, pp. 1421-1434, Dallas.

Disponível em: https://doi.org/10.1145/3133956.3134067 (consultado em 12 de novembro 2017)

UNCTAD (2017), *World Investment Report 2017 – Investment and the Digital Economy*, Geneva, United Nations Publication.

Disponível em: http://unctad.org/en/PublicationsLibrary/wir2017_en.pdf

WEF (2014), "Risk and Responsibility in a Hyperconnected World", *Insight Report*, (online), Janeiro, World Economic Forum.

Disponível em: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

WEF (2016), "The Future of Jobs – Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution", *Global Challenge Insight Report*, (online), Janeiro, World Economic Forum.

Disponível em: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf (consultado em 17 de janeiro 2018).

WEF (2018), *The Global Risks Report 2018, 13th Edition*, Geneva, World Economic Forum.

Disponível em: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (consultado em 17 de janeiro 2018).

Weishäupl, Eva, Emrah Yasasin e Guido Schryen (2018), "Information security investments: An exploratory multiple case study on decision-making, evaluation and learning", *Computers & Security*, February, no prelo.

Disponível em: https://www.researchgate.net/publication/322865436_Information_Security_Investments_An_Exploratory_Multiple_Case_Study_on_Decision-Making_Evaluation_and_Learning (consultado em 19 de abril 2018)

Zigler, Dov (2017), "A Return to Political Economy (Review Essay: The Rise and Fall of American Growth: The U.S. Standard of Living since the Civil War by Robert J. Gordon)", *American Affairs*, Volume I, 1, pp.82–98.

Disponível em: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

ANEXOS

ANEXO A - Guião de entrevista a investigadores e peritos

- *Vantagens e riscos da transformação digital para as empresas (económicos, sociais)?*

- *Perante o quadro nacional e internacional de incentivos (formais: políticos, financeiros; e informais: competitividade, risco financeiro, exposição mediática, etc.) que incentivos faltam para a construção de uma cultura de cibersegurança nas empresas?*

- *Está a Academia a preparar pessoas para responder aos desafios (técnicos, gestores, decisores) nestas matérias?*

    - *A abordagem à cibersegurança e à gestão de risco é multidisciplinar (para além de IT e legislação)?*
    - *Qual a motivação para a Investigação (e formação) nestas áreas? (incentivos políticos, eg programa de educação, iniciativa das Universidades, resposta das Universidades à procura – alunos/empresas, etc.)*
    - *Uniformização curricular ou discricionária?*

- *Em matéria de sensibilização e de formação para os riscos de segurança digital, são ainda em maior número aquelas as organizações que não desenvolvem ações junto dos colaboradores por forma a criar uma consciência para a sua ação, para os riscos e para a reação (AP2SI, 2016; Cardoso, et al., 2017), parecendo existir uma concentração da responsabilidade de gestão das atividades focadas nos riscos de segurança digital nos departamentos e áreas cuja responsabilidade é a da gestão das TIC (AP2SI, 2016; Cardoso, et al., 2017; KPMG, 2018; MARSH, 2018). Estas duas variáveis, sem a possibilidade de se estabelecer uma relação direta, poderão inferir uma maior aposta por parte das organizações numa transformação digital assente, talvez exclusivamente, em estratégias de informatização com pouca ou inexistente correlação com as outras áreas funcionais (Hess, et al., 2016).*

    - *Que razões poderão estar na origem desta concentração nos departamentos de TI? (operacionalização, racionalização de custos, escassez de recursos humanos, etc.)*

- *Que papel tem (ou deve ter) a Academia nos processos de decisão (políticas públicas) nestas matérias?*

- *Que papel deve desempenhar o Estado (regulador, regulamentador, etc.) em matérias de cibersegurança?*

    - *Em que áreas (apoios financeiros, sensibilização, formação, etc.) deve intervir?*
    - *Se não desempenha qualquer papel, qual a razão?*

ANEXO B - Guião de entrevista AP2SI

- *Na perspetiva da AP2SI, e considerando a sua missão, quais as que considera serem as principais vantagens e riscos da transformação digital para as empresas?*

- *Sendo que a AP2SI tem por missão "contribuir para o desenvolvimento da Segurança da Informação em Portugal, de forma ativa, através da sensibilização para o valor e necessidade de proteção da Informação, e do desenvolvimento e promoção de orientações que visem reforçar o conhecimento e a qualificação dos indivíduos e organizações":*
    - *Que perceção tem a AP2SI sobre o nível de conhecimento ou de consciencialização das empresas para os riscos, nomeadamente, sobre a segurança do risco digital? (a perceção entre os seus membros e também de não membros através das ações que vai desenvolvendo, nomeadamente pelo facto de ter já desenvolvido um Inquérito Aberto à Segurança da Informação das Instituições em Portugal)*
    - *Perante o quadro nacional e internacional de incentivos (formais: políticos, financeiros; e informais: competitividade, risco financeiro, exposição mediática, etc.) que incentivos considera a AP2SI que faltam para a construção de uma cultura de cibersegurança nas empresas?*
    - *Que iniciativas têm as Associações desenvolvido nesta matéria junto das empresas? Resultam de iniciativa própria ou como resposta a alguma política pública?*
    - *Considerando as mais recentes iniciativas em Portugal em matéria de cibersegurança - como a instalação de um Centro Nacional de Cibersegurança ou a adoção da Estratégia Nacional de Segurança no Ciberespaço -, assim como na União Europeia - a adoção da Diretiva de Segurança das Redes e da Informação, sensibilização para a cibersegurança no Mercado Único Digital -, bem como as iniciativas que a própria AP2SI tem desenvolvido, que expectativas tem para o segundo Inquérito Aberto à Segurança da Informação das Instituições em Portugal em termos de consciencialização em matérias de cibersegurança (perceção dos riscos, implementação de modelos de gestão de risco, dotação orçamental, etc.)*
    - *Quando será expectável a publicação do segundo Inquérito Aberto à Segurança da Informação das Instituições em Portugal?*

- *Que tipo de envolvimento (coordenação, participação, consulta, etc.) têm ou teve a AP2SI em processos de decisão de políticas públicas nestas matérias?*
    - *(que participação teve a AP2SI no desenvolvimento de políticas públicas nos exemplos dados em ou na Proposta de Lei n.º 119/XIII que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União, etc.)*
    - *O envolvimento que têm ou tiveram foi o que consideram adequando? Ou não tendo tido qualquer envolvimento que papel a AP2SI considera que deveria desempenhar nestes processos?*

- *Há estudos que apontam para uma maior aposta por parte das organizações (empresas) numa transformação digital assente, quase exclusivamente, em estratégias de informatização com pouca ou inexistente correlação com as outras áreas funcionais:*

- *No entendimento da AP2SI, que razões poderão estar na origem desta concentração nos departamentos de TI? (operacionalização, racionalização de custos, escassez de recursos humanos, etc.)*

- *A AP2SI considera que a Academia estará a preparar pessoas (técnicos, gestores, decisores) convenientemente para responder aos desafios nestas matérias (da transformação digital das organizações e da segurança do risco digital?*

- *Na perspetiva da AP2SI, que papel deve desempenhar o Estado, em especial o Governo, em matérias de cibersegurança (regulador, regulamentador, etc.)? E em que áreas considera que deverá intervir e como (apoios financeiros, sensibilização, formação, etc.)?*
  (pode existir correlação com 2b))

ANEXO C - Guião de entrevista a decisores públicos e peritos sobre incentivos

- *Vantagens e riscos da transformação digital para as empresas (económicos, sociais)?*

- *Na edição número 29 do "Ponto de Situação Sistemas de Incentivos às Empresas Portugal 2020", com dados reportados a 30 de novembro de 2017, é possível observar que das 29 216 candidaturas no sistema de incentivos para as empresas, apenas 952 foram submetidas por grandes empresas e as restantes 28 264 submetidas por PME representando, em termos de projetos aprovados, cerca de 80% dos incentivos (COMPETE 2020, 2017:8)*
  Que tipo de incentivos estão disponíveis para a transformação digital?
    - *Existe algum foco destes incentivos na cibersegurança (aplicações e sistemas, formação ou contratação de pessoas)?*

- *Qua a percepção do [organismo público] sobre a acção das empresas, nomeadamente as PME, em matérias de cibersegurança?*
    - *É uma preocupação no momento de optar pela transformação digital?*

- *Que iniciativas são desenvolvidas pelo [organismo público] nesta matéria (cibersegurança) junto das empresas? (Para além dos seminários [identificados], promovidos pelo [organismo público])*

- *Desenvolvem-se estudos nesta área (autónomos, contratados) para suportar as políticas públicas de fomento da transformação digital?*

- *Perante o quadro nacional e internacional de incentivos (formais: políticos, financeiros; e informais: competitividade, risco financeiro, exposição mediática, etc.) que incentivos entende que faltarão e poderão contribuir para a construção de uma cultura de cibersegurança nas empresas?*

- *Que tipo de envolvimento (coordenação, participação) teve o [organismo público] no processo de decisão (políticas públicas) em matérias de cibersegurança? (ENSC – o CSSC só surge posteriormente)*
    - *Qual o papel que deveriam desempenhar nestes processos?*

- *Entende que a Academia está a preparar pessoas para responder aos desafios (técnicos, gestores, decisores) nestas matérias?*
- *Que papel deve desempenhar o Estado (regulador, regulamentador, etc.) em matérias de cibersegurança?*

- *Em que áreas (apoios financeiros, sensibilização, formação, etc.) deve intervir?*
- *Se não desempenha qualquer papel, qual a razão?*

ANEXO D - Guião de entrevista CNCS

- *Sendo que a Resolução do Conselho de Ministros n.º 12/2012 que define implementação de uma estratégia global da Administração Pública na área das TIC, atribuiu ao GNS a "Definição e implementação de uma estratégia nacional de segurança da informação" (Medida 4) e tendo os termos do funcionamento do CNCS no âmbito do GNS sido estabelecidos em 2014 (Decreto-Lei n.º 69/2014, de 9 de maio), se existiu, qual foi o envolvimento do CNCS na elaboração da Estratégia Nacional de Segurança no Ciberespaço em 2015?*

    - *As propostas para a ENSC resultaram de avaliações, estudos, pareceres técnicos internos? Foram auscultadas/consultadas organizações (públicas ou privadas, associações representativas ou individuais)?*

    - *Foram auscultados/consultados investigadores e peritos (especialmente sobre modelos, conceitos e políticas públicas)? Que áreas de investigação/científicas foram envolvidas?*

    - *Que tipo de instrumentos de consulta foram utilizados?*

- *Do conjunto de competências atribuídas ao CNCS (Decreto-Lei n.º 69/2014, de 9 de maio), todas elas de grande relevância, há duas que gostaria de destacar no âmbito deste trabalho:*

    - *«b) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança»;*

    - *«g) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança»*

    - *No âmbito destas competências, que acções desenvolve e que instrumentos utiliza o CNCS que visem a formação e qualificação de pessoas e a promoção de projectos de inovação e desenvolvimento nesta matéria?*

    - *A APDC, no seguimento de um evento reservado que realizou, relata a existência de "57 protocolos com entidades privadas" (estabelecidos pelo CNCS). Confirma-se a existência destes protocolos e o seu enquadramento nestas atribuições do CNCS?*

- *A ENSC «funda-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas».*
  No seu pilar da subsidiariedade atribui uma hierarquia de responsabilidades na segurança do ciberespaço, iniciando-se «no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais», atribuindo ao sector privado a «responsabilidade primária pela sua proteção».

- *Neste quadro de «responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais», que instrumentos o CNCS identifica como estando definidos para avaliar e gerir «de forma adequada» os riscos inerentes ao ciberespaço, «assegurando-se a proporcionalidade dos meios e medidas para o seu exercício» (pilar da proporcionalidade)?*

- *Não obstante o foco praticamente exclusivo da ENSC em medidas com vista à proteção de infraestruturas críticas nacionais , o seu Eixo 4 – Educação, sensibilização e prevenção, é determinado que devem ser promovidas «campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas» e «estabelecer programas específicos para as Pequenas e Médias Empresas (PME), para as associações socioprofissionais e, em particular, para os profissionais liberais».*

    - *Neste âmbito, e dado que ao CNCS é atribuído um papel de coordenação operacional, relativamente às entidades públicas e às infraestruturas críticas (Eixo 1 – Estrutura de segurança do ciberespaço), que papel e intervenção tem o CNCS, ou é chamado a ter, em medidas definidas no referido Eixo 4?*

        - *Que papel e intervenção tem junto dos cidadãos?*

        - *Que papel e intervenção tem junto das empresas?*

- *Tendo a ENSC sido aprovada em Maio 2015 com «prazo máximo de três anos» para a sua revisão e «verificação anual dos objetivos estratégicos e das linhas de ação e adequação dos mesmos à evolução das circunstâncias», e em 2017 sido constituído o grupo de projeto denominado Conselho Superior de Segurança do Ciberespaço (CSSC) que tinha «por missão assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da respetiva revisão»*

    - *No entendimento do CNCS, que razão ou razões existirão para não serem conhecidos publicamente quer um plano de ação para a sua implementação (entendido como «medidas concretas e respetivas linhas de ação» que "enformam" os seis objetivos estratégicos) ou resultados das mencionadas verificações anuais?*

- *Recentemente foi aprovada a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico do ciberespaço (transpondo a Diretiva NIS de 2016), em resultado da apresentação de uma proposta coordenada pelo CNCS (ou GNS?).*

    - *As propostas para esta Lei resultaram de avaliações, estudos, pareceres técnicos internos? Foram auscultadas/consultadas organizações (publicas ou privadas, associações representativas ou individuais)?*
    - *Foram auscultados/consultados investigadores e peritos (especialmente sobre modelos, conceitos e políticas públicas)? Que áreas de investigação/científicas foram envolvidas?*

    - *Que tipo de instrumentos de consulta foram utilizados?*

- *Recentemente foi aprovada a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico do ciberespaço (transpondo a Diretiva NIS de 2016), em resultado da apresentação de uma proposta coordenada pelo CNCS (ou GNS?). Considerando que:*

    - *Pela Lei, para além dos operadores de infraestruturas críticas, ficam também abrangidos operadores de serviços essenciais e os prestadores de serviços digitais, excluindo grande parte do tecido económico português do seu âmbito e do conjunto de incentivos (coercivos) que estabelece, isto é, isentando aqueles que não se enquadrem nos parâmetros definidos para operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, mas que, por serem maioritariamente do setor privado, são reconhecidos pelo papel que desempenham na economia e na segurança do ciberespaço;*

    - *Não entende o CNCS que objetivo primeiro do CSSC, o de «assegurar a coordenação político-estratégica para a segurança do ciberespaço», poderá estar de alguma forma comprometido uma vez que, apesar do alargamento da sua uma composição, continua a excluir o setor privado de um papel mais ativo e interventivo em prol do aprofundamento da «segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.»?*

      (refira-se que a nova formação retira ao presidente do CSSC a capacidade de convidar para «participar nos trabalhos do CSSC representantes indicados por outras entidades, bem como personalidades de reconhecido mérito na área em que são desenvolvidos os trabalhos» e estabelece agora que, «por sua iniciativa ou a pedido de qualquer dos membros do Conselho, [o presidente] pode convocar outros titulares de órgãos públicos ou convidar outras personalidades de reconhecido mérito para participar em reuniões do Conselho Superior de Segurança do Ciberespaço")

- *Estando anunciado processo de elaboração de uma nova ENSC, e assumindo que a sua preparação foi coordenada pelo CNCS (ou GNS?) e respeitando a anterior composição do CSSC,*

    - *As propostas para a nova ENSC resultaram de avaliações, estudos, pareceres técnicos das entidades que constituem o CSSC? Foram auscultadas/consultadas organizações (publicas ou privadas, associações representativas ou individuais)?*
    - *Foram auscultados/consultados investigadores e peritos (especialmente sobre modelos, conceitos e políticas públicas)? Que áreas de investigação/científicas foram envolvidas?*

    - *Que tipo de instrumentos de consulta foram utilizados?*

- *Recentemente (maio 2018) o CNCS coordenou um ciberexercício de âmbito nacional para avaliar o estado de preparação das entidades participantes.*

    - *Este exercício contou com a participação de empresas?*

- *Que tipo de empresas e setores estiveram representados (infraestruturas críticas)?*
- *Que critérios foram adotados na escolha das empresas que participaram?*
- *Que instrumentos de disseminação foram utilizados (direcionados, públicos, etc.)?*

- *O CNCS dispõe de competências, métodos ou instrumentos que permitam proceder a avaliações ou análises com o objetivo de traçar um quadro nacional como base para sustentar e apoiar a decisão e as políticas públicas em matérias de cibersegurança e do impacto da transformação digital nas organizações?*
  (estudos de impacto, de análise e gestão do risco, indicadores, etc.)

- *No seu papel de «assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança», bem como na (eventual) relação que tem com as organizações, em especial as empresas, o CNCS identifica ou considera que existe uma atenção aos aspetos relacionados com a cibersegurança (uma cultura de cibersegurança) por parte das empresas e dos gestores? (é uma temática preocupa as organizações ou é uma temática ainda sem expressão ou sem relevância para estas?)*

- *Considerando que a cultura de cibersegurança numa empresa está diretamente relacionada com a cultura organizacional, perante o quadro nacional e internacional de incentivos (formais: políticos, financeiros; e informais: competitividade, risco financeiro, exposição mediática, etc.) na perspetiva do CNCS, que incentivos considera faltarem para a construção de uma cultura de cibersegurança nas organizações e na empresas?*
  (Mais sensibilização? Por quem? Mais formação de empresários, gestores, quadros? Mais investimento? Etc.)

- *Em matéria de sensibilização e de formação para os riscos de segurança digital, são ainda em maior número aquelas as organizações que não desenvolvem ações junto dos colaboradores por forma a criar uma consciência para a sua ação, para os riscos e para a reação (AP2SI, 2016; Cardoso, et al., 2017), parecendo existir uma concentração da responsabilidade de gestão das atividades focadas nos riscos de segurança digital nos departamentos e áreas cuja responsabilidade é a da gestão das TIC (AP2SI, 2016; Cardoso, et al., 2017; KPMG, 2018; MARSH, 2018). Estas duas variáveis, sem a possibilidade de se estabelecer uma relação direta, poderão inferir uma maior aposta por parte das organizações numa transformação digital assente, talvez exclusivamente, em estratégias de informatização com pouca ou inexistente correlação com as outras áreas funcionais (Hess, et al., 2016).*
  - *No entendimento do CNCS, que razões poderão estar na origem desta concentração da responsabilidade pela segurança da informação e cibersegurança nos departamentos de TI? (entendimento dos gestores de que estes temas pertencem "à informática", por questões de operacionalização, racionalização de custos, escassez de recursos humanos, etc.)*

- *Considera o CNCS que a Academia a preparar pessoas para responder aos desafios (técnicos, gestores, decisores, empresários) nestas matérias?*

- *Na perspetiva do CNCS, que papel deve desempenhar o Estado, em especial o Governo, em matérias de cibersegurança (regulador, regulamentador, etc.)? E em que áreas* considera que deverá intervir e como (apoios financeiros, sensibilização, formação, etc.)?

ANEXO E – Referências sobre cibersegurança em páginas de Internet das Associações e Confederações empresariais

Este exercício de pesquisa foi realizado, em todas as páginas, no dia 12 de abril de 2018 e repetido no dia 25 de maio de 2018. Em 12 de abril de 2018 apenas obtivemos resultados na página da COTEC. Em 25 de maio de 2018 foi possível obter resultados na página da COTEC e também da CIP.

CIP – Confederação da Indústria Portuguesa:

"Business Europe discute cibersegurança" (fonte: http://cip.org.pt/businesseurope-discute-ciberseguranca/ consultado em 25 de maio de 2018)

COTEC Portugal - Associação empresarial para a Inovação:

"A cibersegurança tem de ter um racional de negócio" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/a-ciberseguranca-tem-de-ter-um-racional-de-negocio/ consultado em 25 de maio de 2018)

"Uma parte da segurança digital não tem a ver com tecnologia. Tem a ver com pessoas" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/uma-parte-da-seguranca-digital-nao-tem-a-ver-com-tecnologia-tem-a-ver-com-pessoas/ consultado em 25 de maio de 2018)

"A Transformação Digital requer um reforço da Cibersegurança" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/a-transformacao-digital-requer-um-reforco-da-ciberseguranca/ consultado em 25 de maio de 2018)

"Boa cibersegurança é sinónimo de bons negócios" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/boa-ciberseguranca-e-sinonimo-de-bons-negocios/ consultado em 25 de maio de 2018)

"Como inovar para combater o cibercrime?" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/como-inovar-para-combater-o-cibercrime/ consultado em 25 de maio de 2018)

"Especialistas internacionais em cibersegurança vêm a Portugal" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/especialistas-internacionais-em-ciberseguranca-vem-a-portugal/ consultado em 25 de maio de 2018)

"Innovation Meets Cybersecurity: the public-private cooperation challenge (Lotação esgotada)" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/innovation-meets-cybersecurity-the-public-private-cooperation-challenge/ consultado em 25 de maio de 2018)

"Associados da COTEC reúnem-se para testar Ciber-resiliência" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/associados-da-cotec-reunem-se-para-testar-ciberresiliencia/ consultado em 25 de maio de 2018)

"COTEC presente na Conferência Anual de Cibersegurança" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/cotec-presente-na-conferencial-anual-de-ciberseguranca/ consultado em 25 de maio de 2018)

"COTEC e CNCS cooperam no âmbito da promoção da cibersegurança" (fonte: http://www.cotecportugal.pt/pt/noticias-e-eventos/cotec-e-cncs-cooperam-no-ambito-da-promocao-da-ciberseguranca/ consultado em 25 de maio de 2018).

ANEXO F – Legislação consultável em matéria de segurança nacional com relação à segurança na Internet

"Regime de proteção jurídica dos programas de computador" (Decreto-Lei n.º 252/94, Diário da República n.º 243/1994, Série I-A de 1994-10-20 e respetivas alterações, disponível em http://data.dre.pt/eli/dec-lei/252/1994/p/cons/19971127/pt/html)

"Proteção jurídica das bases de dados" (Decreto-Lei n.º 122/2000, Diário da República n.º 152/2000, Série I-A de 2000-07-04, disponível em http://data.dre.pt/eli/dec-lei/122/2000/07/04/p/dre/pt/html)

"Lei de Combate ao Terrorismo" (Lei n.º 52/2003, Diário da República n.º 193/2003, Série I-A de 2003-08-22 e respetivas alterações, disponível em http://data.dre.pt/eli/lei/52/2003/p/cons/20150624/pt/html)

"Serviços da sociedade de informação, em especial do comércio eletrónico" (Decreto-Lei n.º 7/2004, Diário da República n.º 5/2004, Série I-A de 2004-01-07 e respetivas alterações, disponível em http://data.dre.pt/eli/dec-lei/7/2004/p/cons/20120829/pt/html)

"Lei de Segurança Interna" (Lei n.º 53/2008, Diário da República n.º 167/2008, Série I de 2008-08-29 e respetivas alterações, disponível em http://data.dre.pt/eli/lei/53/2008/p/cons/20170524/pt/html)

"Lei do cibercrime" (Lei n.º 109/2009, Diário da República n.º 179/2009, Série I de 2009-09-15, disponível em http://data.dre.pt/eli/lei/109/2009/09/15/p/dre/pt/html)

"Procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes e transpõe a Directiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro" (Decreto-Lei n.º 62/2011, Diário da República n.º 89/2011, Série I de 2011-05-09, disponível em http://data.dre.pt/eli/dec-lei/62/2011/05/09/p/dre/pt/html)

"Orientação para a política de Ciberdefesa" (Despacho n.º 13692/2013, Diário da República n.º 208/2013, Série II de 2013-10-28, disponível em https://dre.pt/application/conteudo/3295679)

"Estratégia Nacional de Combate ao Terrorismo" (Resolução do Conselho de Ministros n.º 7-A/2015, Diário da República n.º 36/2015, 1º Suplemento, Série I de 2015-02-20, disponível em http://data.dre.pt/eli/resolconsmin/7-a/2015/02/20/p/dre/pt/html).

Sobre proteção de dados pessoais e comunicações eletrónicas ver https://www.cncs.gov.pt/recursos/legislacao/dados-pessoais-e-comunicacoes-electronicas/.