INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Comunicação sobre cibersegurança em contexto de teletrabalho nas agências de marketing digital

Bruna Alexandra Batalha dos Santos

Mestrado em Comunicação, Cultura e Tecnologias da Informação

Orientador:
Doutor Pedro Miguel Pereira Neto, Professor Auxiliar Convidado,
Iscte – Instituto Universitário de Lisboa

Novembro, 2021

SOCIOLOGIA
E POLÍTICAS PÚBLICAS

Departamento de Sociologia

Comunicação sobre cibersegurança em contexto de teletrabalho nas agências de marketing digital

Bruna Alexandra Batalha dos Santos

Mestrado em Comunicação, Cultura e Tecnologias da Informação

Orientador:
Doutor Pedro Miguel Pereira Neto, Professor Auxiliar Convidado
Iscte – Instituto Universitário de Lisboa

Novembro, 2021

Dedicado aos meus avós: Maria da Conceição, Maria Teresa e António Carlos,

Por todo o amor, força, incentivo e carinho inesgotável

E por serem os meus perenes exemplos de bondade, lealdade e perseverança.

AGRADECIMENTOS

A concretização da presente dissertação foi um processo longo e desafiante a vários níveis. Ainda assim, não tenho quaisquer dúvidas em como todo este processo seria muito mais penoso sem os conselhos, o apoio e a motivação que senti ao longo de todos estes meses.

A Deus, por todos os momentos em que não me senti só, pela fé inabalável na conclusão deste projeto e por me permitir terminá-lo, mesmo com todos os desafios que estiveram no meu caminho.

Ao Professor Pedro Pereira Neto, por todas as sugestões e conselhos e por ter sido uma inspiração em cada instante enquanto professor de mestrado e orientador.

Aos meus pais, Ana e António, pelo amor, raízes humildes e bons princípios que sempre me incutiram. Por todo o seu esforço para que eu tivesse sempre mais estudos e conhecimentos sobre o mundo.

Aos meus avós, que serão sempre os melhores avós do mundo, e que sempre apoiaram incondicionalmente todos os meus sonhos e projetos de vida, procurando que crescesse não só de forma mais sábia como de forma mais bondosa.

Ao meu namorado, Nuno, pelo amor inesgotável, pelo carinho e motivação ao longo de todos estes anos. Por compreender e aceitar todos os momentos em que não estive tão presente, em prol deste estudo.

Aos meus amigos, especialmente à Alícia, à Eva, à Filipa, à Patrícia, ao Nuno e ao Sérgio, por todos os momentos de partilha, suporte emocional e esclarecimento de dúvidas.

Às empresas e respetivos colaboradores que aceitaram participar neste estudo, disponibilizando o seu tempo para responderem a todas as minhas questões e que possibilitaram a conclusão com sucesso desta etapa académica.

RESUMO

Um universo digitalmente interligado não é necessariamente um universo mais seguro: a pandemia de Coronavírus tornou o digital um alvo ainda maior para os hackers, levando a um aumento do número de ataques em empresas de vários setores, particularmente devido ao crescimento do número de indivíduos em teletrabalho.

Assim, através de uma análise da literatura existente sobre esta temática e dos dados provenientes de entrevistas semiestruturadas a membros de agências de marketing digital portuguesas, este estudo procura compreender como está a ser realizada a comunicação sobre cibersegurança e quais os efeitos colocados pela atual pandemia.

Palavras-chave: Cibersegurança, Teletrabalho, Comunicação, Pandemia de COVID-19, Marketing Digital

ABSTRACT

A digitally interconnected universe is not necessarily safer: the Coronavirus pandemic has made the digital an even bigger target for hackers, leading to an increase in the number of attacks in companies across industries, particularly due to the rise of individuals in remote work.

Thus, through an analysis between the existing literature on this topic and data from semi-structured interviews with Portuguese digital marketing members, this study seeks to understand how communication on cybersecurity is being carried out in practice and what are the effects of the current pandemic.

Keywords: Cybersecurity, Remote work, Communication, COVID-19 pandemic, Digital marketing

For every lock there is someone out there trying to pick it

or break in.

David A. Bernstein

ÍNDICE

GLOSSÁRIO DE SIGLAS

BBC — British Broadcasting Corporation

CERT.PT — Computer Emergency Response Team

CNCS — Centro Nacional de Cibersegurança

CNPD — Comissão Nacional de Proteção de Dados

ENSC — Estratégia Nacional de Segurança do Ciberespaço

EUA — Estados Unidos da América

GNS — Gabinete Nacional de Segurança

ILO — International Labour Organization

INE — Instituto Nacional de Estatística

ONU — Organização das Nações Unidas

QNRCS — Quadro Nacional de Referência para a CiberSegurança

RGPD — Regulamento Geral de Proteção de Dados

SSI — Sistema de Segurança Interna

TIC — Tecnologias da Informação e da Comunicação

VPN — Virtual Private Network

UE — União Europeia

INTRODUÇÃO

Ao longo dos anos, e graças ao contínuo desenvolvimento tecnológico, a Internet tem vindo a ganhar cada vez mais um papel de destaque na sociedade, sendo usada pela comunidade científica e educacional como ferramenta indispensável para a rápida disseminação de informação sobre variados temas, e permitindo o crescimento de áreas vitais como a energia, os transportes, as comunicações, o comércio e as finanças (Lipson, 2002).

Contudo, a contínua massificação do uso da Internet, bem como o aparecimento mais recente de aplicações e outros serviços de gestão da rede, não chegam a todos os pontos do globo terrestre da mesma forma, impossibilitando os habitantes de terem as mesmas igualdades de acesso ao digital: “Embora a sua globalização seja evidente e tenha permitido uma taxa de abrangência à escala mundial, é ainda possível encontrar zonas do globo que, por ordem política ou outras, não dispõem de acesso à Internet” (Antunes e Rodrigues, 2018: 5).

Para além das razões de ordem política supracitadas, podemos ainda considerar as questões sociais, como a própria recetividade e literacia de cada indivíduo para o uso da Internet (Wen Gong *et. al*, 2007), e as questões culturais de cada região do globo, as quais explicam as diferenças existentes no uso e acesso à Internet em vários países.

Atualmente, podemos também considerar a pandemia de Coronavírus (Covid-19) como outro fator de exclusão digital, contribuindo para que instituições de vários setores recorram ao teletrabalho para atenuar os seus efeitos nefastos. Segundo dados do INE (2020), o segundo trimestre de 2020 ficou marcado pelo crescimento de 23,1% do número de pessoas em teletrabalho, representando 1,094 milhões de teletrabalhadores. Desse número, a larga maioria (91,2%) indicou que o principal motivo pelo qual exerciam as suas funções remotamente era a pandemia.

Entre as instituições que mais recorreram ao teletrabalho estão as de marketing digital que, pelas suas caraterísticas – recurso em grande escala às tecnologias e plataformas digitais (websites, blogs, e-mail e redes sociais, por exemplo) como bases essenciais para o seu funcionamento - beneficiam de uma maior facilidade na adaptação a este novo regime de trabalho. Contudo, segundo Manokha (2020), a impossibilidade de recorrer ao teletrabalho em todos os setores da indústria pode originar uma divisão entre os indivíduos que são beneficiados e os que são excluídos por esse mesmo processo.

Além disso, a pandemia representa ainda uma ameaça à proteção dos dados pessoais, registando-se entre fevereiro e março de 2020 um aumento dos ciberataques (CNCS, 2020a), os quais usam a velocidade e conetividade global da Internet para se disseminarem de forma

mais eficaz pelas redes, deixando poucas evidências que possam ser usadas para identificar os atacantes (Lipson, 2002).

Assim, este estudo pretende compreender qual a possível ligação entre a pandemia de Covid-19, a cibersegurança e a comunicação, analisando como foi a passagem para o teletrabalho e quais as principais dificuldades sentidas pelos colaboradores e administração das agências de marketing digital, encontrando-se organizado da seguinte forma:

O Capítulo I reunirá alguma literatura sobre a vigilância, com especial incidência na relação existente entre as sociedades atuais e o digital, bem como a sua relação com a privacidade, explorando diversas teorias e conceitos, como o Panóptico, Sociedade em Rede e Vigilância Lateral.

O Capítulo II abordará a cibersegurança e o controlo no mundo laboral, procurando elucidar o leitor sobre algumas das principais ameaças em contexto de teletrabalho, bem como um resumo sobre o atual quadro regulatório nacional e comunitário. Este capítulo incluirá ainda algumas das possíveis estratégias usadas para diminuir a vulnerabilidade dos sistemas informáticos.

O Capítulo III apresentará a metodologia escolhida para a recolha de dados sobre o tema, a qual passa pela realização de entrevistas a membros da administração e funcionários de agências do setor de marketing digital, contribuindo de forma positiva para o conhecimento existente sobre este tema.

No Capítulo IV será discutida a análise dos resultados e as principais conclusões alcançadas através da metodologia usada.

Por fim, o Capítulo V apresentará algumas considerações finais, as quais pretendem resumir os resultados alcançados e sugerir propostas de trabalho futuro nesta área.

1. VIGILÂNCIA

1.1. Sociedade digital

O advento das novas tecnologias e do seu impacto na sociedade iniciou-se com as inúmeras inovações tecnológicas desenvolvidas no âmbito da 2ª Guerra Mundial, as quais foram posteriormente alvo de melhorias contínuas ao longo dos anos, permitindo a criação de dispositivos eletrónicos cada vez mais eficientes.

A importância que este desenvolvimento tecnológico assumiu, nomeadamente a nível dos países desenvolvidos, originou uma tentativa de vários autores para, ao longo dos anos, definirem e caraterizarem as respetivas sociedades, suportadas pelo digital.

Daniel Bell (1973) foi um dos pioneiros na criação do conceito de *Sociedade da Informação*, um conceito adequado para definir a sociedade pós-industrial, caraterizada pelo avanço tecnológico particularmente nos serviços de informação, os quais, por sua vez, passaram a requerer maiores qualificações por parte dos trabalhadores. Isto traduziu-se num favorecimento do trabalho intelectual em detrimento do trabalho manual, diminuindo a classe operária. Bell (1973) divide ainda a sociedade em três espaços distintos e autónomos: estrutura social, política e cultura. Segundo Frank Webster (1995), o facto destes serem completamente autónomos uns dos outros permite a Bell evitar questões ligadas a possíveis relações entre eles sendo esse facto algo que, para Webster, deita por terra a teoria de Bell: "os serviços expandiram-se para garantir uma economia estabelecida e interconectada, bem como relações políticas e culturais mais amplas"[1] (Webster, 1995: 50).

Como sugestão, Webster (1995) sugere uma divisão da sociedade da informação segundo cinco critérios: tecnológico, económico, ocupacional, espacial e cultural, os quais permitem distingui-la de todas as outras sociedades. Contudo, o autor (ibid, 1995) afirma que é difícil definir a partir de que ponto a sociedade da informação se formou, até porque foi esta que se adaptou aos avanços tecnológicos realizados e não o contrário.

Um outro conceito criado foi o de *Sociedade em Rede*, a qual pode ser definida enquanto sociedade que se apoia nas redes tecnológicas como uma nova forma de organização social, manifestando-se de variadas formas conforme a cultura e a história de cada sociedade (Castells e Cardoso, 2006). Mas mesmo nos dias atuais é possível observar que o desenvolvimento tecnológico não chegou a todos os continentes da mesma forma, não sendo possível dar a todos os indivíduos as mesmas oportunidades de acesso ao digital nem as mesmas vantagens que advêm desse mesmo acesso, pelo que este conceito não pode ser aplicado de forma generalizada:

[1] Tradução livre.

> The global networking of society by new media gives us an impression of the overall wealth and innovative capacities of contemporary society. However, due to the colonization of society by the instrumental reason of competition, new achievements remain limited to certain classes and don't benefit all (Fuchs, 2008: 270).

Contudo, Fuchs (2008) afirma que a sociedade não é algo estático: é mutável, moldada pelo próprio ser humano como resultado da sua influência sobre o que o rodeia. Seguindo essa linha de pensamento e estando a sociedade tão intrinsecamente ligada às novas tecnologias, principalmente a partir do final do séc. XX, assiste-se aos impactos desta ligação tanto na vida pessoal como profissional dos indivíduos (Pedro, 2014).

Um conceito mais recente para caracterizar as sociedades contemporâneas é o de *Platform Society*, da autoria de Van Dijck, Poell e De Waal (2018). Segundo estes autores, o que carateriza esta sociedade é precisamente o envolvimento da mesma com as TIC, permitindo às relações sociais serem o foco ao invés da economia, motivo pelo qual este conceito seria dos mais apropriados para definir a sociedade atual:

> That is why we prefer the term "platform society"— a term that emphasizes the inextricable relation between online platforms and societal structures […] The "platform society" does not merely shift the focus from the economic to the social; the term also refers to a profound dispute about private gain versus public benefit in a society where most interactions are carried out via the Internet (Van Dijck, Poell e De Waal, 2018: 2).

De entre as maiores vantagens e atividades desenvolvidas pelas TIC e na própria Internet, destacam-se: a rapidez no tratamento e processamento de informação, o fortalecimento de relações de cariz profissional e social, o acesso a conteúdo didático e de entretenimento, e ainda a Internet das Coisas [2](Antunes e Rodrigues, 2018).

Segundo Weber e Studer (2016) é precisamente esta conexão global que, através da implantação na rede de dispositivos insuficientemente protegidos, alterou o cenário dos ciberataques, potenciando um aumento dos riscos e das vulnerabilidades a nível da cibersegurança destes dispositivos e das próprias atividades que os utilizadores desenvolvem no digital. Entre outros impactos negativos da Internet salientamos ainda como principais exemplos: dependência, défice de atenção, diminuição da capacidade do indivíduo para tomar decisões e deterioração das relações sociais (Quaglio e Millar, 2020).

[2]No original, *Internet of Things*, termo criado por Ashton (1999), é definida como uma infraestrutura globalmente conectada onde os objetos do dia-a-dia são os elementos principais. cf (Atzori et. al., 2016) "Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm", *Ad Hoc Networks*, 56

Segundo o CNCS (2019: 12), é devido à premissa de que "(…) os elementos tecnológicos são robustos e fiáveis e que tecnologias emergentes e complexas têm o potencial para oferecer uma elevada flexibilidade e eficiência na comunicação" que se torna fulcral garantir níveis mais elevados de cibersegurança — uma tarefa nem sempre fácil, como se verá ao longo deste estudo.

Para Fuchs (2008), um dos maiores problemas originados por uma sociedade digital reside não na tecnologia em si, mas no facto de esta tornar a sociedade cada vez mais competitiva e menos cooperativa – algo que, segundo o autor se deve procurar combater, ainda que este admita que esse é um processo que exigiria do ser humano uma vontade e necessidade vitais para se reorganizar.

1.2. Privacidade na sociedade vigilante

Embora não seja algo novo, os estudos sobre esta temática e a sua importância para as sociedades têm crescido ao longo dos anos, de modo particular desde a perda de privacidade dos cidadãos e das empresas originada pelo aumento da vigilância nas redes (Antunes e Rodrigues, 2018). De facto, grande parte desses estudos aborda a privacidade e a segurança, mostrando que estes conceitos não podem ser dissociados (Dal Bello, 2011; Andrade, 2013; Estêvão, 2014; Lyon, 2018; Stallings e Brown, 2018). Sendo a vigilância um fenómeno complexo, é possível encontrar várias tentativas de autores para defini-la enquanto conceito (Estêvão, 2014):

Para Fuchs (2010) a vigilância pode ser definida enquanto recolha e armazenamento de dados de pessoas singulares ou coletivas, com o objetivo de exercer sobre estas controlo e disciplina. De modo particular, em relação à vigilância online, acrescenta ainda que esta é altamente opaca para os utilizadores devido à complexidade dos processos que a envolvem, os quais tornam praticamente impossível para o utilizador saber onde ficam armazenados os seus dados e quais os indivíduos que têm acesso aos mesmos (ibid, 2011: 145).

Lyon (1998, apud Estêvão, 2014), divide a vigilância em três formatos, os quais possuem fins distintos: 1) vigilância pela entidade patronal; 2) vigilância de segurança e policiamento; e 3) vigilância para fins comerciais, sendo que para este estudo consideramos como particularmente relevantes o primeiro e terceiro formato.

É ainda possível considerar o conceito de Vigilância Lateral como um quarto formato (Estêvão, 2014), o qual encontra nas sociedades tecnológicas o seu expoente máximo de atuação, onde o indivíduo simultaneamente vigia e é vigiado, num sistema que continua a seguir a visão panóptica de Foucault, embora seja necessária uma contextualização atual (Espanha e Estêvão, 2017).

Rosa e Chevitarese (2017) concordam com esta visão, defendendo que redes sociais como Facebook e Snapchat são o novo Panóptico da Sociedade em Rede pois permitem não só que algumas organizações – por exemplo, agências de marketing – façam uso da recolha de dados para fins comerciais, como ainda a existência uma vigilância por parte da rede de conexões que se vai criando ao longo do tempo nelas.

Pelas suas caraterísticas, a vigilância encontra-se ainda ligada aos estudos sobre o poder das sociedades e dos indivíduos que as constituem. Entre esses estudos, o Panóptico[3] é geralmente usado como maior exemplo (Foucault, 1999; Andrade, 2013; Rosa e Chevitarese, 2017). Mais tarde, Foucault (1999) acabou por atribuir ao Panóptico um outro significado, associando-o à punição e a sanções normativas através das quais o indivíduo é coagido a adotar comportamentos corretos por relações de poder dentro de uma sociedade que Foucault designa como *disciplinar*.

Para Deleuze (1992: 216), a sociedade disciplinar veio a ser substituída pela sociedade de controlo, a qual funciona "(…) não mais por confinamento, mas por controle contínuo e comunicação instantânea". Para o Estado a vigilância é uma ferramenta fundamental, não só para a organização da sociedade como ainda para prevenir desastres e calamidades como o 11 de Setembro (Andrade, 2013). Ou seja, a sociedade continua a seguir um padrão de controlo, mas agora considerando que a vigilância é necessária para o bem-estar e prevenção (Lyon, 2018).

Segundo Pedro (2014) viver em sociedade acarreta para o individuo algumas condições, entre as quais se destaca o facto da sua intimidade não ser, de modo algum, inviolável — uma perspetiva partilhada por Webster (1995):

> Put in less abstract terms, if we as a society are going to respect and support the individuality of members, then a requisite may be that we know a great deal about them. For instance, if each of us, as an individual, is to have a vote, then we must be individuated at least by name, age and address (Webster, 1995: 54).

Por esse motivo, embora reconhecida a sua importância e vantagens, a vigilância é associada a uma ideia negativa precisamente pelo controlo exercido e falta de privacidade (Fuchs, 2011; Andrade, 2013), acentuados pelo aparecimento da Internet e das redes sociais. Contudo, Andrade (2013: 28) afirma que estas questões acentuam o "clássico problema da privacidade: como então equilibrar os custos e benefícios?". A autora (ibid: 2013) acrescenta que mesmo que o ser humano esteja disposto a sacrificar voluntariamente a sua privacidade

[3] Concebido por Jeremy Bentham (1785), designa a "prisão ideal", onde um único vigilante poderia controlar todos os prisioneiros, através da vigilância exercida sobre estes e da arquitetura do próprio edifício, o qual permitiria ao vigilante vigiar sem ser visto.

pelo prazer ou vantagens do uso das tecnologias continua a correr um risco sério: a impossibilidade de controlar aquilo que os outros farão com os seus dados.

A privacidade pode ser definida enquanto algo presente em todas as relações sociais, sendo da responsabilidade de cada indivíduo a delimitação dos limites sociais, físicos, psicológicos ou informativos (Trepte, 2015), desempenhando um papel fundamental na dignidade humana, ao garantir a salvaguarda não só das nossas desgraças mas também da nossa capacidade de pensar, falar e agir do mesmo modo quando nos encontramos sozinhos (Payton e Claypoole, 2014).

A privacidade pode ainda corresponder à "delimitação de um espaço físico – a casa, o quarto, a casa de banho" (Andrade, 2013), com o objetivo de manter o nível de respeito que cada indivíduo merece (Payton e Claypoole, 2014), sendo um direito fundamental do ser humano[4].

A fusão de tecnologia, computação e comunicação com vários aspetos da nossa vida pode assim, para além dos benefícios, apresentar-nos novos desafios de segurança e privacidade, principalmente no digital (Trappe e Straub, 2018), embora nem sempre exista concordância entre os autores. Por um lado, o conceito de *Platform Society* defende que o uso das redes sociais, longe de criar uma revolução, representa uma nova forma de interação entre os indivíduos, constituindo uma relação inseparável entre o online e as estruturas sociais (Van Dijck, Poell e De Waal, 2018), e permitindo aos seus utilizadores a criação de uma pegada digital a partir do armazenamento de um vasto número de informações que podem ser de cariz privado ou não. Por outro lado, Antunes e Rodrigues (2018) acrescentam que a Internet possibilitou que qualquer individuo com acesso tenha informação sobre outras pessoas, identificando algumas das possibilidades das redes sociais – como a partilha de fotos e identificação dos utilizadores permitida pelo Facebook – como um comportamento que viola a privacidade.

Payton e Claypoole (2014) sugerem que as nossas pesquisas online acabam por ser mais valiosas do que se pensa, uma vez que muitas delas dão mais informação que aquela que daríamos num telefonema ou mensagem, definindo a privacidade como essencial na manutenção do controlo sobre as nossas escolhas: quanto maior a nossa privacidade, maior a nossa capacidade para não permitirmos que terceiros tenham influência sobre nós e as nossas ações, atuando assim como forma de proteção (Rossoni e Bolesina; 2014). É essa proteção que nos permite apresentarmo-nos aos outros da forma como desejamos que os outros nos vejam (Payton e Claypoole, 2014).

[4] Artigo 12º da Declaração Universal dos Direitos Humanos: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei" (ONU,1948). Disponível em: https://unric.org/pt/declaracao-universal-dos-direitos-humanos

Na perspetiva de Lyon (2018) foi precisamente o advento das redes sociais — a par com outros eventos marcantes do séc. XXI — a impulsionar a *Cultura de Vigilância* que marca a atualidade. E são as caraterísticas desta cultura — diversidade, fluidez e imprevisibilidade — que contribuem para que as sociedades contemporâneas precisem de estar cada vez mais atentas e formadas para os desafios que a tecnologia acarreta.

É ainda necessário ressalvar que embora a expansão da Internet potencie formas mais tradicionais de ciberataque por parte de hackers – como por exemplo, a cópia dos dados do cartão de crédito para usos não autorizados – uma análise a diversos serviços em nuvem pode levar a informações ainda mais confidenciais e que, à partida, não suspeitamos que sejam tornadas públicas. Um exemplo disso são os dispositivos de segurança que algumas casas e empresas instalam, por forma a monitorizar qualquer problema que possa existir e que coloque em risco o bem-estar de quem se encontrar nesse local, ou proteger objetos valiosos, por exemplo, de um assalto (Payton e Claypoole, 2014; Trappe e Straub, 2018). Segundo Trappe e Straub (2018), este tipo de serviços acaba também por registar os movimentos dos indivíduos e as suas atividades pessoais, ultrapassando a esfera da privacidade pessoal e familiar.

Por esse motivo Andrade (2013: 29) defende que o poder do individuo reside na sua decisão para "(…) não divulgar ou revelar muitas informações sobre si", acabando por manter a sua liberdade de escolha. Soares, Araújo e Souza (2020) apontam como exemplo a política de privacidade existente em várias redes sociais e aplicações, e cujo objetivo é informar o utilizador sobre a recolha dos dados, finalidade e durante quanto tempo estes serão armazenados. No entanto, esse documento é intencionalmente ambíguo, vago e extenso, pelo que a maioria dos utilizadores limita-se a concordar com os termos, sem qualquer interesse em ler as condições (Soares, Araújo e Souza, 2020).

Nesse sentido, parece-nos importante referir o Paradoxo da Privacidade[5], termo usado para indicar uma oposição entre a intenção e o comportamento real do utilizador (Kokolakis, 2017). Contudo, este conceito não é isento de controvérsia pois nem sempre a intenção e o comportamento divergem, em todos os utilizadores, em todos os momentos (ibid, 2017).

Outro dos estudos mais relevantes sobre privacidade é o da Teoria dos Círculos Concêntricos[6], ainda que esta levante uma série de problemas e questões principalmente

[5] No original, XXX, a primeira utilização deste termo é atribuída a Norberg et al. (2007), que dirigiu um estudo com uma amostra de estudantes, o qual demonstrou que o indivíduo tende a revelar mais dados consoante a sua perceção de risco. Cf. Kokolakis (2017),"Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon" *Computer and Security* vol. 64, pp.122-134

[6] Criada por Heinrich Hubmann, em 1953, é ainda conhecida como Teoria das Esferas. Segundo esta teoria, a vida privada de cada individuo pode ser dividida em três círculos concêntricos: a privacidade, como o círculo exterior, englobaria as relações interpessoais e de interesse público, não permitindo um grande nível de conhecimento sobre a vida do indivíduo; no círculo intermédio da intimidade existiria um certo nível de sigilo, mais profundo que o da privacidade, onde se inserem informações

devido à subjetividade dos conceitos de intimidade e privacidade, os quais variam segundo os aspetos culturais e pessoais de cada indivíduo (Rossoni e Bolesina, 2014). Assim, por não existir uma clareza suficiente na definição da fronteira entre todos estes círculos, torna-se importante a criação e aplicação de leis sobre este tema, de modo a procurar-se uma uniformização sobre os direitos e deveres dos cidadãos. Nem sempre isto é fácil: a própria legislação sobre o direito à privacidade e os usos da informação privada não são os mesmos nem têm as mesmas aplicações em todos os países. Embora os Estados Unidos da América protejam determinados tipos de informação pessoal, como por exemplo contas bancárias, registo de cuidados de saúde e toda a informação sobre menores de idade, existe uma valorização dos interesses pessoais e governamentais em detrimento da privacidade de cada cidadão para prevenir ataques terroristas, pelo que informações como a nossa localização geográfica, compras online ou visitas a websites são controladas e não têm caráter privado. Por outro lado, na União Europeia e países como o Canadá e o México, a informação de caráter pessoal e sensível pertence unicamente à pessoa a quem essa informação se refere – e não à pessoa que detém posse dessa mesma informação (Payton e Claypoole, 2014).

Uma pesquisa da BBC (2010) indicou que apesar de 49% dos utilizadores da Internet à escala mundial sentirem que esta não é um local seguro para expressarem as suas opiniões e de 20% temer as ameaças à privacidade, continua a existir uma resistência considerável (53%) à regulamentação da Internet, contribuindo para acentuar as dificuldades na implementação de leis. Embora Payton e Claypoole (2014) defendam a necessidade de colocar limites à recolha e armazenamento de dados, sugerindo a criação de leis para esse efeito, a dúvida permanece: seria possível garantir, com toda a segurança, que essas leis estariam seriam cumpridas por todos os indivíduos da mesma forma? O contínuo avanço tecnológico e expansão da Internet tornam impossível dar esta garantia, motivo pelo qual se torna necessário alertar cada vez mais os indivíduos para o risco da exposição a novos perigos, garantindo ao mesmo tempo que esses não deixam de fazer uso e tirar o melhor proveito possível de todas as vantagens que as novas tecnologias oferecem.

partilhadas com menos pessoas; por fim, o círculo do segredo, caraterizado como sendo o mais interno e profundo, guarda todas as informações que não são compartilhadas com os outros. cf Caroline Rossoni e Iuri Bolesina (2014). “A Teoria dos Círculos Concêntricos e a Proteção à Vida Privada: Análise ao Caso Von Hannover vs. Alemanha, Julgado pela Corte Europeia de Direitos Humanos” *XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea – VII Mostra de Trabalhos Jurídicos Científicos*

2. CIBERSEGURANÇA EM TELETRABALHO – ATUALIDADE

2.1. Ameaças

A globalização e a grande velocidade dos avanços tecnológicos tornaram uma parte da sociedade cada vez mais dependente da tecnologia e, por esse motivo, mais vulnerável às ameaças que os utilizadores podem encontrar no digital: segundo Stallings e Brown (2018: 627) "a expansão das comunicações e interconexões trazidas pela Internet aumentam o poder do indivíduo para causar danos"[7].

Por esse motivo, torna-se importante não apenas adotar políticas de cibersegurança que vão de encontro ao contínuo desenvolvimento tecnológico como garantir a sensibilização dos utilizadores da Internet para essas mesmas políticas e ameaças:

> O espírito aberto e descentralizado com que a Internet foi crescendo e acolhendo todas as pessoas e instituições, não lhes impondo qualquer "direito de admissão", permitiu que nela fossem entrando os mais diversos tipos de utilizadores e com as mais variadas motivações (Antunes e Rodrigues, 2018: 69).

Embora existam várias definições sobre o que é a cibersegurança, para efeitos do presente estudo usaremos a definição referida por Antunes e Rodrigues (2018: 103): "O termo cibersegurança engloba as ações de monitorização, prevenção e neutralização das ameaças que possam pôr em risco a liberdade dos cidadãos e das empresas, bem como o bem-estar socioeconómico das nações".

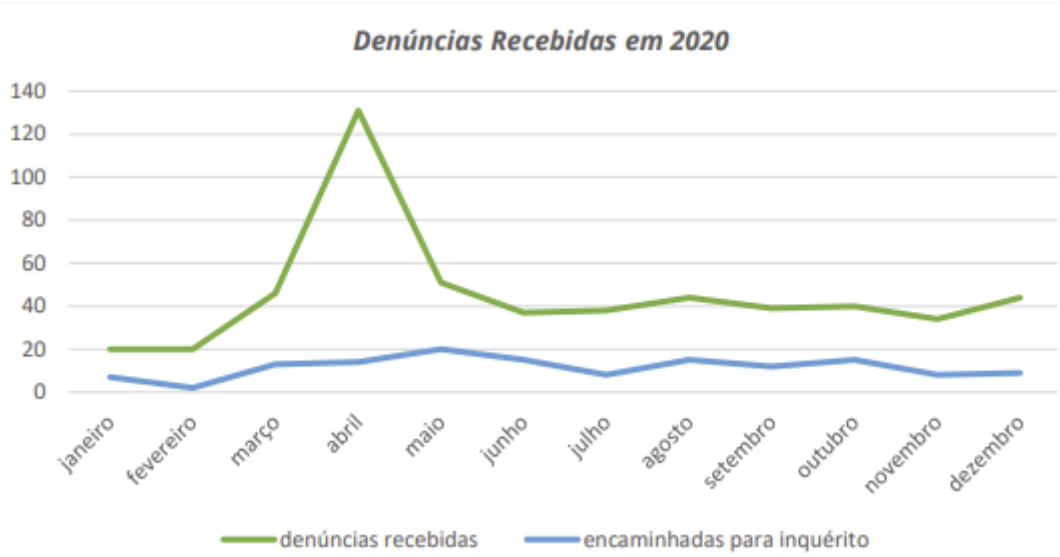
Os estudos realizados revelam um consenso quanto à relação entre o digital e a sociedade com o aumento dos cibercrimes, algo acentuado nos últimos anos, como indica Matos (2018):

> 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 (Matos, 2018: 1).

[7] Tradução livre.

Só em 2020 registou-se um aumento do número de denúncias de cibercrimes em território nacional, num período coincidente com o aparecimento da pandemia de Coronavírus em Portugal (ver Figura 2.1.), uma relação justificada pelo "(…) incremento do tempo de utilização do ambiente digital, o incremento do teletrabalho e a consequente diluição da tradicional segurança perimétrica das organizações" (SSI, 2020: 159).

Figura 2. 1 – Denúncias recebidas em 2020, das quais se salienta o elevado aumento no período compreendido entre fevereiro e maio.



Fonte: Ministério Público – Gabinete de Cibercrime (2021), Nota Informativa: Cibercrime – Denúncias Recebidas 2020. (8 de janeiro). Consultado em: 15.04.2021. Disponível em: https://cibercrime.ministeriopublico.pt/pagina/cibercrime-em-2020-denuncias-recebidas

Para o CNCS (2020d: 23), "As organizações, em particular as empresas, são um dos atores mais importantes do ciberespaço, visto constituírem grande parte do tecido económico". Desse modo, o aumento do cibercrime colocou ainda mais pressão nos especialistas e departamentos de cibersegurança de várias empresas e organizações por todo o mundo.

É importante salientar que, embora usada com conotação negativa, *hacking*[8] não é, por si só, considerado ato ilegal, excetuando nos casos em que "comprometa a segurança de um computador ou de uma rede informática sem o prévio consentimento do seu proprietário" (CNCS 2020c: 32). Contudo e independentemente do grupo[9] onde os seus praticantes sejam

[8] Termo usado para referir a invasão ilícita e o acesso não autorizado aos sistemas informáticos, com o objetivo de recolher informações importantes sobre o funcionamento dos mesmos. cf. Antunes e Rodrigues (2018), *Introdução à Cibersegurança: A Internet, os Aspectos Legais e a Análise Digital Forense*, 1ª ed. FCA – Editora de Informática

[9] O *hacking*, bem como os seus praticantes e atividades desenvolvidas podem classificar-se em dois grupos distintos: *hacking* ético (White Hat), o qual não causa danos nos sistemas informáticos ou mesmo nas próprias empresas, e *hacking* não ético (Black Hat), responsável pela provocação de danos, incluindo roubo ou espionagem, para a obtenção de benefícios em prol dos seus praticantes. cf. (ibid)

incluídos, as atividades desenvolvidas, ou mesmo a tentativa de as desenvolver, através do hacking "podem constituir um crime de acesso ilegítimo e punível por lei" (Antunes e Rodrigues, 2018: 107).

Entre os principais cibercrimes praticados em 2020 estão *phishing*[10], *malware*[11], *ransomware*[12], intrusão e fraude/ burla (CNCS, 2021) (ver Quadro 2.1).

Quadro 2. 1 - Tabela dos principais incidentes informáticos registados pelo CERT.PT em 2020 por comparação a 2019.

2019				2020*					Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	% C/V	% S/V	Tendência absoluta %	Lugar RK
1º	*Phishing/smishing*	236	31	1º	*Phishing/smishing*	613	43	46	+ 160	=
2º	Infeção (*malware*)	123**	16	2º	Sistema infetado (*malware*)	169	12	13	+ 37	=
3º	Compromisso de Conta	95	13	3º	Distribuição de *malware*	119	8	9	+ 116	+
4º	Exp. de vuln. (intrusão)	58	8	4º	Compromisso de conta não privilegiada	111	8	8	N/A	N/A
5º	Distribuição (*malware*)	55	7	5º	Acesso não autorizado	58	4	4	+ 867	+
6º	Tentativa de *login*	30	4	6º	Compromisso de aplicação	55	4	4	N/A	N/A
7º	*Scan*	28	4	7º	Sistema vulnerável (vulnerabilidade)	41	3	N/A	N/A	N/A
8º	DoS/DDoS	27	4	8º	Utilização Ilegítima de nome de terceiros	32	2	2	+ 68	+
9º	Utilização ilegítima de nome de terceiros	19	3	9º	Indeterminado (outro)	28	2	2	+ 65	+
10º	Exp. de vuln. (tentativa de intrusão)	18	2	10º	Tentativa de *login*	26	2	2	- 13	-

Fonte: CNCS (2021), Relatório Cibersegurança em Portugal: Riscos e Conflitos. Consultado em 10.05.2021. Disponível em: https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2021__observatoriociberseguranca_cncs.pdf

De entre estes cibercrimes consideramos como particularmente relevantes para este estudo os que têm a engenharia social como base (*phishing* e intrusão) devido à componente social e comunicativa na origem das suas técnicas, provando que comportamentos de risco levam a falhas de segurança e estas, por si, levarão à criação de condições de vulnerabilidade que podem permitir um ciberataque (Baptista, 2017). A engenharia social, ou seja, o ato de manipular um indivíduo com o objetivo de levá-lo a executar uma ação que pode ou não ser do seu interesse, incluindo a obtenção de informações ou acesso não solicitado (Hadnagy,

[10] Mensagens enviadas através de e-mail, SMS ou chat com o objetivo de levar os destinatários a fornecer informações confidenciais. Cf. Antunes e Rodrigues (2018), *Introdução à Cibersegurança – A Internet, os Aspetos Legais e a Análise Digital Forense*, 1ª edição, FCA – Editora de Informática.

[11] Conhecido como "Software Malicioso" é um programa introduzido num sistema informático sem conhecimento do utilizador e cujo objetivo é perturbar a vítima através do dano causado ao próprio sistema, às aplicações e aos dados. Cf. CNCS (s.a), *Glossário*. Disponível em: https://www.cncs.gov.pt/pt/glossario/#linhasobservacao

[12] Faz parte da categoria de malware e destina-se a inoperalizar o sistema informativo da vítima, levando esta a receber pedidos de resgate para recuperar o acesso. Cf. CNCS (s.a), *Glossário.* Disponível em: https://www.cncs.gov.pt/pt/glossario/#linhasobservacao

2011), é um exemplo de cibercrime que assenta no comportamento humano como a principal vulnerabilidade de qualquer sistema informático, algo já referenciado em outros estudos:

> A História ensinou-nos que ataques de engenharia social são extremamente eficientes para obter acesso não autorizado a informação sensível. Uma das vantagens da engenharia social é que os utilizadores geralmente gostam de ajudar e serem úteis e assim acabam por fornecer informação sensível apenas porque lhes perguntaram (Mendes, 2014: 7).

Para Abass (2018) hoje em dia grande parte das empresas investe muito dinheiro na compra de dispositivos de segurança quando, na prática, um atacante que utilize a engenharia social precisa não de um elevado conhecimento técnico mas sim de astúcia e inteligência, de forma a tirar partido do fator humano:

> Today most business and banks are relying on technology like internet and smartphone. They are paying a lot of money for buying security tools software and hardware, but at the same time a naïve employer can give all the information the attacker need without going to the trouble of hacking the system. That is what social engineering all about use the human factor which is the weakest factor in any institute or organization. Humans are easier to hack than computer systems and networks. Most people are raised to be kind and helpful leading them to inherently trust others. The concept of bad people taking advantage of the good and honest does not sit well with most people (Abass, 2018: 258).

Neste tipo de crimes, e particularmente em entidades que baseiam a sua atividade no digital, é comum o roubo de identidade, principalmente de indivíduos ligados à Direção[13] (CNCS 2021; Baptista, 2017), de modo a persuadirem as suas vítimas a cederem dados de acesso ao sistema interno da organização. De entre as técnicas de engenharia social mais usadas nas redes sociais Antunes e Rodrigues (2018: 53) destacam: a criação de um perfil falso mas credível, através do qual o atacante procura obter informações de cariz pessoal e/ou confidencial; e promoção de ciberataques, particularmente *phishing* e a partilha de conteúdos falsos pelos contactos existentes no perfil da vítima, fazendo-se passar por esta.

Para Hadnagy (2011) o grande poder da engenharia social está na forma como o hacker faz uso da sua comunicação com o alvo. Baseando-se nos modelos de comunicação de

[13] Também referido como *CEO Fraud*.

Shannon e Weaver[14], bem como de Berlo[15], Hadnagy (2011) defende que a preocupação de um *hacker* que use engenharia social deverá ser a transmissão de uma mensagem que vá de encontro aos interesses do recetor/ alvo, para que este possa sentir-se interessado e motivado em prolongar a comunicação, permitindo assim que o hacker entre no seu espaço pessoal com maior facilidade.

A atual pandemia aumentou os níveis de ansiedade dos indivíduos, tornando-os especialmente vulneráveis a e-mails, mensagens e telefonemas relacionados com o Coronavírus, uma vulnerabilidade da qual os cibercriminosos se aproveitaram, tendo crescido o número de mensagens e websites falsos que imitam autoridades e outras fontes confiáveis (Pranggono e Arabo, 2020). No caso português, o CNCS (2020b) emitiu um alerta aconselhando "(…) extrema prudência no acesso, na receção e na partilha de conteúdos digitais associados à temática da pandemia COVID-19", e onde destaca como principais ciberameaças relacionadas ao Coronavírus: campanhas de *phishing*, divulgação de aplicações e plataformas digitais (Covid-19 Tracker), *crowdsourcing* para falsas campanhas de aquisição de material médico e de proteção, e divulgação de SMS indicando a necessidade de pagamento de determinados valores que serão posteriormente reembolsados pelo Estado, no âmbito das medidas aplicadas para contenção da pandemia (CNCS, 2020b).

Além disso, as dificuldades na regulamentação e fiscalização das leis sobre cibercrime bem como "a preocupação com a segurança da organização e responsabilidade civil"[16], levam os indivíduos a não reportar tanto os ciberataques (Stallings e Brown, 2014: 614).

2.2. Controlo digital no mundo do trabalho

A vigilância não é algo exclusivo do teletrabalho[17]: numa sociedade onde a tecnologia impera, as empresas e empregadores encontram nos meios de vigilância uma forma de controlo sobre os seus funcionários, monitorizando o seu comportamento. E aqui entende-se como meios de vigilância não só as câmaras como ainda telefones, correio eletrónico, o GPS e a própria

[14] A Teoria Matemática da Comunicação (1948), proposta por Shannon e Weaver foi criada no âmbito da Segunda Guerra Mundial, e exemplifica a forma como as mensagens podem ser transmitidas de forma mais eficiente e no menor tempo possível, graças a processos de codificação/ descodificação de sinais por parte do emissor e do recetor, respetivamente. cf. C.E.Shannon (1948), "A Mathematical Theory of Communication" *The Bell System Technical Journal*, 27, pp. 379-423, 623-656, July, October.

[15] Segundo David Berlo (1958), a comunicação pode ser definida enquanto uma interação entre duas pessoas, no mínimo, e onde estas partilham um mesmo conjunto de sinais e regras que lhes permitem compreender a informação trocada entre si. cf. David Hadnagy (2011), *Social Engineering – The Art of Human Hacking,* Wiley Publishing Inc., Indianapolis, Indiana.

[16] Tradução livre.

[17] "Considera-se teletrabalho a prestação laboral realizada com subordinação jurídica, habitualmente fora da empresa e através do recurso a tecnologias de informação e de comunicação" cf. Artigo 165º *Lei nº7/2009, Diário da República n.º 30/2009, Série I de 2009-02-12*, Código do Trabalho.

Internet (Pedro, 2014). Embora tanto o RGPD como a lei portuguesa [18]defendam a proibição do uso de meios eletrónicos de vigilância à distância para controlar o desempenho profissional do trabalhador, este mesmo uso continua a ser permitido quando a sua finalidade é a proteção e segurança das pessoas e bens, devendo o empregador informar sobre a existência e finalidade destes meios no local de trabalho.

A pandemia de Coronavírus obrigou a passagem para o teletrabalho em vários setores onde existia essa viabilidade. Apesar de ter sido bem recebida na maior parte dos países, a esperada continuidade do teletrabalho em níveis massivos no futuro levanta algumas preocupações, entre elas a contribuição para um padrão irregular de trabalho, onde os funcionários devem encontrar-se constantemente disponíveis, levando à dissolução da fronteira entre a vida privada e o trabalho, e contribuindo para uma forma de alienação da realidade (Manokha, 2020). No caso do teletrabalho as orientações emitidas pela CNPD (2020) indicam que embora o empregador mantenha os poderes que lhe são associados, continua a ser proibida a utilização de meios de videovigilância neste regime, salvaguardando assim a privacidade do trabalhador, da sua família e do seu lar.

Ainda que o teletrabalho apresente as suas vantagens, entre elas um maior aumento da flexibilidade dos funcionários, uma redução dos custos para as empresas e dos custos de mobilidade (Fairweather, 1999; Belzunegui-Eraso e Erro-Garcés, 2020), também apresenta desvantagens, tais como: extensão da vigilância laboral para o ambiente familiar dos funcionários (Manokha, 2020), falta de clareza em relação a prioridades ou tarefas a realizar, sobrecarga, enviesamento da comunicação e ainda fadiga, irritabilidade, sentimento de exclusão e stress (ILO, 2020). Além disso, existe ainda um acréscimo das despesas relativas à eletricidade, telefone e Internet em casa, gerando alguma controvérsia sobre a extensão do disposto no Artigo 168º do Código do Trabalho (2009)[19], o qual afirma que o empregador deve assegurar o pagamento de despesas subordinadas ao teletrabalho, bem como da instalação e manutenção de equipamentos, salvo quando estipulado em contrato.

Fairweather (1999) defende que apesar de existir algum interesse por parte dos empregadores para esta extensão da vigilância continua a existir espaço para alguma privacidade, uma vez que na relação empregador-empregado não se incluem contextos onde exista necessidade de revelar informações de caráter mais intimista.

---

[18] Artigo 20º da Lei n.º 7 de 2009, *Diário da República n.º 30/2009, Série I de 2009-02-12*, Código do Trabalho

[19] "Na falta de estipulação no contrato, presume-se que os instrumentos de trabalho respeitantes a tecnologias de informação e de comunicação utilizados pelo trabalhador pertencem ao empregador, que deve assegurar as respectivas instalação e manutenção e o pagamento das inerentes despesas." Cf. Lei nº7/2009, *Diário da República n.º 30/2009, Série I de 2009-02-12*, Código do Trabalho. Disponível em: https://dre.pt/web/guest/legislacao-consolidada/-/lc/168156178/202110111132/74211789/diploma/indice

Para Manokha (2020) a vigilância no local de trabalho é uma necessidade estrutural do capitalismo, pois torna-se necessário garantir que o trabalho é realizado da forma mais eficiente possível. Assim, o teletrabalho criou a necessidade de encontrar novas formas de garantir esta mesma eficiência fora do local de trabalho, pois o horário laboral pertence ao empregador uma vez que este paga um determinado número de horas diárias ao funcionário (ibid: 277).

De ressalvar que, independentemente dos métodos de vigilância usados, todos eles se caraterizam pela entrada do empregador no espaço privado de outrem (ibid: 281), pelo que se salienta o reforço que deve existir no cuidado com as informações recolhidas. Numa Sociedade em Rede, o controlo não é absoluto e todos são suscetíveis de cometer erros (Andrade, 2013) pelo que não apenas a comunicação sobre a vigilância e cibersegurança deve ser efetuada com maior clareza e objetividade, como deve garantir-se que todos os indivíduos estão cientes das consequências que uma relação custo-benefício com as novas tecnologias pode acarretar.

2.3. Quadro regulatório nacional e comunitário

Apesar do aumento das preocupações com o reforço de regras comuns e princípios sobre cibersegurança por parte dos Estados-Membros da UE, parece existir alguma resistência à criação de um tratado internacional sobre esta matéria, em grande parte por se acreditar que "a regulação do ciberespaço não deve ser feita por meio de regras jurídicas vinculativas, mas sim por meio de recomendações e compromissos políticos", sendo a sua adesão por parte dos Estados e outras entidades voluntária (CNCS 2020c :9). Contudo, salienta-se que embora as estratégias desenvolvidas passem por linhas orientadoras diferentes, o seu objetivo é essencialmente o mesmo: proteção da informação, segurança do ciberespaço e o incentivo para a continuidade da cooperação internacional (Baptista, 2017).

No caso europeu, embora a preocupação com a cibersegurança exista desde a década de 90, apenas em 2016 a UE adotou aquele que seria o seu primeiro ato legislativo sobre esta temática: a Diretiva 2016/ 1148, com o objetivo de uniformizar o nível de segurança das redes e da informação em todos os Estados-Membros (CNCS 2020c). Ainda na UE, atualmente aplica-se o Regulamento do Parlamento Europeu e do Conselho (2019), o qual remete para a competência de cada Estado-Membro o controlo e aplicação das leis relativas à cibersegurança, referindo ainda a necessidade do reforço da sensibilização das pessoas e organizações para este tema, devido à sua intrínseca ligação com o comportamento humano. Mais recentemente, no final de 2020, a UE adotou uma nova Estratégia de Cibersegurança para a Década Digital, com vista à implementação de soluções globais a nível da

cibersegurança e procurando reforçar a cooperação, a segurança e a prevenção neste domínio (EU, 2021).

Em Portugal, a autoridade nacional para a certificação da cibersegurança denomina-se Centro Nacional de Cibersegurança (CNCS), a qual atua no âmbito do Gabinete Nacional de Segurança (GNS) junto de entidades do Estado e outros operadores, de forma a garantir o cumprimento da legislação e, desse modo, que o uso do ciberespaço é sinónimo de segurança, liberdade e justiça para os seus utilizadores. Juntamente com o CNCS, atua ainda o CERT.PT, serviço responsável pela resposta a acidentes de cariz informático no ciberespaço nacional.

Para além das políticas públicas nacionais seguirem as diretrizes da U.E., a Lei nº 109/ 2009 (15 de setembro) é reconhecida enquanto referência em matéria de cibercrime – sendo ainda designada como Lei do Cibercrime – segundo a qual os cibercrimes podem ser punidos com penas que podem ir desde uma multa a pena de prisão até 10 anos, nos casos mais graves. Para além disso, em 2015 foi ainda aprovada em Conselho de Ministros a primeira Estratégia Nacional de Segurança do Ciberespaço, a qual foi posteriormente revogada e reformulada para 2019-2023:

> A ENSC 2019-2023 assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. (…) A consecução da ENSC 2019-2023 permitirá tornar Portugal um país mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade (Resolução do Conselho de Ministros nº 92/ 2019).

Contudo, subsistem dúvidas sobre a sua aplicação, principalmente na sua articulação com o Código de Processo Penal, "(…) em virtude da área de sobreposição existente entre o artigo 189.º do Código e os artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 19.º (interceção de comunicações) da Lei do Cibercrime." (CNCS 2020c: 102), um obstáculo que é necessário ultrapassar na formulação de futuras leis sobre este tema. Sobre isto, Matos (2018: 17) realça a importância de investir na renovação das políticas públicas tendo por base não os indicadores disponíveis mas sim o aprofundamento dos "processos de avaliação que permitam compreender como e de que forma esses indicadores de execução foram influenciados por políticas anteriores".

Merece ainda destaque a dificuldade do cidadão comum no entendimento das leis: embora Antunes e Rodrigues (2018: 96) afirmem que "não é missão do cidadão comum, que apresenta uma queixa de um crime de que foi alvo, saber interpretar as leis", os autores concordam sobre os benefícios que essa interpretação teria, não apenas no entendimento geral dos cidadãos sobre o percurso penal de um processo como ainda no contributo para um

maior sentido de “cidadania, mais conhecimento e, em certa medida, mais prevenção e segurança na utilização da Internet e dos seus serviços” (ibid: 69).

2.4. Estratégias e boas práticas

Embora o Estado desempenhe um papel relevante na defesa dos interesses e na luta contra os desafios de cibersegurança impostos pelo digital (Matos, 2018), não podemos afastar a responsabilidade das empresas na proteção dos seus colaboradores, dados e sistemas informáticos. Boas políticas de cibersegurança são fundamentais para prevenir ciberataques, bem como para uma melhor gestão da situação no caso destes ocorrerem.

O surgimento da pandemia criou duas prioridades imediatas para as empresas: garantir que as suas equipas estavam preparadas para a passagem de funções para teletrabalho, bem como a continuidade da cibersegurança dos seus dados (Boehm et. al. 2020). De modo geral, “(…) qualquer hacker se vê com acesso a informação sensível, quer de natureza pessoal, quer empresarial, detendo um enorme poder sobre redes, aplicações e sistemas digitais” (CNCS 2020c: 32), pelo que, em primeiro lugar, é fundamental as empresas contratarem profissionais de cibersegurança que demonstrem não só competências técnicas como ainda bons padrões éticos (CNCS 2020c).

No inquérito à “Utilização de Tecnologias da Informação e da Comunicação nas Empresas” [20], realizado em 2020, observa-se que apenas 22,9% das empresas com 10 ou mais colaboradores possui especialistas em IT. Contudo, este número aumenta para 71% em empresas do setor da Informação e Comunicação – onde se incluem as agências de marketing digital. Segundo Matos (2018) é possível que o incentivo à digitalização das empresas seja o principal responsável pela diferença de valores.

Alguns estudos recentes sobre a cibersegurança em teletrabalho indicam ainda que apesar das empresas reconhecerem a segurança da informação como um pilar importante para o seu funcionamento, o fator humano é ainda pouco reconhecido como elemento central na cibersegurança, faltando muitas vezes diretrizes aos funcionários sobre como proceder em caso de ciberataque ou como adotar boas práticas de cibersegurança durante o teletrabalho (Georgiadou et. al., 2021; Wang e Alexander, 2021). Além disso, a implementação de uma cultura de cibersegurança dentro das empresas carece de investimentos financeiros para que se torne mais eficaz e permita uma gestão eficiente dos recursos humanos e técnicos da própria empresa, sendo por esse motivo muitas vezes encarada como uma despesa e não como um investimento (Matos, 2018).

[20] Inquérito anual realizado pelo INE. Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621360&DESTAQUESmodo=2

Devido ao contínuo avanço tecnológico, as ciberameaças não são passíveis de serem eliminadas, mas apenas restringidas (Baptista, 2017). Por esse motivo, acreditamos ser de extrema relevância as empresas e organizações efetuarem uma boa gestão do risco (*risk management*), definido como o processo formal através do qual são definidas as áreas em maior risco de sofrerem um ciberataque, as ciberameaças e os procedimentos necessários para combate-las (Stallings e Brown, 2014). Com efeito, o CNCS (2021) identifica o Insider[21] como um dos principais agentes de ameaça aos sistemas informáticos, com intenções que podem ir desde as mais maliciosas às mais negligentes.

Representando o ser humano um dos maiores fatores de risco para os sistemas informáticos, não podemos abordar *risk management* sem mencionar duas teorias comportamentais, nomeadamente, *Situational Theory of Publics*[22] e *Elaboration Likelihood Model*[23]. Através destas duas teorias podemos compreender a ligação existente entre o comportamento e a vontade do individuo, principalmente quando suportadas pelos sete Princípios da Persuasão[24], através dos quais as pessoas podem ser persuadidas a agir de formas contrárias àquelas que eram as suas intenções iniciais.

Desse modo, torna-se fulcral o desenvolvimento de uma cultura de cibersegurança dentro das empresas, a qual lhes permita desenvolver ações e estratégias para minimizar os riscos e danos de possíveis ciberataques. Embora Matos (2018: 1) defenda que a implementação desta cultura estará sempre condicionada a diversos fatores — tanto de ordem interna como externa — é importante que todos os funcionários, independentemente da posição que ocupam dentro da empresa, estejam cientes das suas responsabilidades e adotem comportamentos ciberseguros (Baptista, 2017):

> A consciência da Cibersegurança deve começar no topo da pirâmide da organização. As funções de administração e de direção intermédia necessitam de ter uma noção

[21] "Agente que coloca em causa a cibersegurança da organização na qual trabalha" CNCS (2021: 76)

[22] Teoria desenvolvida por James E. Grunig em 1968, e segundo a qual é possível segmentar públicos diferentes segundo aquilo que se pretende comunicar, baseando-se em cinco variáveis distintas: capacidade de resposta aos problemas, natureza da comunicação, atitudes e comportamento, relação organização-público e o comportamento coletivo enquanto forma de pressão sobre as organizações. Cf. (Grunig, 2005), "Situational theory of publics" *Theories of Publics and Communication Behavior*, January 2005

[23] Desenvolvida por Richard E. Petty e John Cacioppo, em 1980, foca-se no uso da persuasão como estímulo para a mudança de comportamentos, podendo a persuasão dar origem a comportamentos ponderados e onde a mensagem é recebida com um alto nível de capacidade cognitiva ou, por outro lado, originar comportamentos baseados apenas nas motivações dos indivíduos. Assim, dependendo da forma como os estímulos persuasivos são processados, as mudanças de comportamento podem ser duradouras ou breves. Cf. (Petty e Cacioppo, 1986), "The Elaboration Likelihood Model of Persuasion" *Advances in Experimental Social Psychology* vol. 19, pp. 123-205, December.

[24] Cialdini (1984) afirma que qualquer que seja a estratégia de persuasão usada, esta assenta em 7 princípios-chave: reciprocidade, consistência, prova social, gosto, autoridade, escassez e unidade (tradução livre). Cf. (Cialdini, 2005), "Principles of Persuasion" *Proceedings*

> exata dos riscos, não só para a organização como um todo, mas também como eles próprios podem colocar a organização em risco se não forem cuidadosos. (…) Por outro lado, os trabalhadores das áreas técnicas e de gestão funcional têm um papel diferente, mas altamente influente em apoiar, criar e manter uma organização segura. São eles que podem trazer à gestão de topo das organizações informação técnica atualizada sobre os novos desafios e riscos com que as organizações se defrontam. (…) Por fim, todos na organização necessitam de entender que a segurança da organização depende de todos e de cada um dos funcionários em particular (ibid, 2017: 62).

Michaelides (2020) defende que os comportamentos de cibersegurança adotados em casa são diferentes daqueles adotados no escritório, dada a diminuição da consciência sobre a segurança da informação. Por essa razão, a formação e educação para comportamentos ciberseguros parece constituir, na maior parte dos estudos sobre esta temática, uma das medidas preventivas mais eficazes para levar os cidadãos a tomar consciência das suas responsabilidades em relação às novas tecnologias, assegurando a tomada de comportamentos seguros e conscientes, preservando a sua privacidade e liberdade e garantindo ainda a segurança dos dados que partilham online (Baptista, 2017; Antunes e Rodrigues, 2018; Matos, 2018; CNCS 2020c):

> Os utilizadores da Internet que nasceram após o seu aparecimento nos países desenvolvidos, designados por millennials ou nativos digitais, facilmente se adaptaram à utilização diária destas novas tecnologias. Outros, porém, tiveram que se adaptar com mais ou menos dificuldade a esta nova realidade. Em ambos os casos, é evidente a falta de formação no uso eficiente das tecnologias. Por um lado, por uma eventual falta de interesse individual em investir em formação ao longo da vida, e, por outro, pela rápida e constante evolução tecnológica que tem impossibilitado estratégias de formação adequadas (Antunes e Rodrigues, 2018: 63).

De modo a prevenir ciberataques nas redes sociais, sugere-se a averiguação de perfis que se suspeite serem falsos, evitar qualquer tipo de partilha de informação pessoal e confidencial — mesmo com um utilizador que se saiba ser legítimo — bem como a localização georreferenciada (Antunes e Rodrigues, 2018: 54). Deve ainda avaliar-se cuidadosamente o conteúdo de vídeos e fotos, de modo a prevenir a chantagem e tentativas de extorsão de dinheiro (*sextortion*) (ibid, 2018: 55).

Alguns autores indicam ainda como outras possíveis medidas de cibersegurança em teletrabalho: salvaguardar as infraestruturas, garantindo que os dispositivos de trabalho têm uma ligação VPN forte, bem como antivírus e outras proteções; encorajar os funcionários a recorrerem às equipas de cibersegurança/ informática, de modo a garantir que qualquer

problema técnico seja corrigido da forma mais breve possível; rever periodicamente as configurações de segurança dos principais serviços usados; e reforçar os cuidados no uso do digital, não só nos adultos como nas populações mais jovens, as quais devem usufruir de um conjunto de matérias escolares que lhes permitam desenvolver competências e conhecimentos sobre este tema desde cedo (Antunes e Rodrigues, 2018; Malecki, 2020).

O CNCS disponibiliza de forma atualizada no seu website manuais de boas práticas e orientações de cibersegurança para diversas situações: ensino à distância, teletrabalho, viagens, pagamentos online e campanhas eleitorais. Procura ainda fomentar a sensibilização dos cidadãos para esta temática, tanto através da disponibilização de alertas de segurança como através de ações de formação e cursos, como é o caso dos programas "Cidadão Ciberseguro" e "Cidadão Ciberinformado". No caso dos jovens, e de modo a reforçar o seu envolvimento em cibersegurança, destacam-se ainda as exposições, publicação de conteúdos e outras atividades decorridas no âmbito do dia da "Internet Segura". Salienta-se ainda a Iniciativa Portugal INCoDE.2030, cujo objetivo principal passa pelo reforço das competências digitais dos cidadãos, tanto através do investimento na qualificação dos jovens como nos recursos humanos, ações estas planeadas para o período de tempo compreendido entre 2017 e 2030.

Segundo Matos (2018: 69), um maior envolvimento do Estado português e a coordenação deste "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" seria uma das possíveis estratégias de cibersegurança a ser implementada a nível nacional, tanto em empresas de domínio público como privado. É igualmente importante um maior investimento em recursos, tanto de ordem técnica como humana, sendo estes últimos dos mais importantes para uma aplicação bem-sucedida das leis (Stallings e Brown, 2018).

Outras propostas a nível nacional incluem "programas de capacitação e formação de cidadãos e trabalhadores em cibersegurança" (Baptista, 2017: 48), o aprofundamento científico do conceito de Engenharia Social e de outros ciberataques (Mendes, 2014) de modo a implementarem-se estratégias cada vez mais fortes e capazes de os combater, e ainda a criação e implementação, em todas as organizações públicas e privadas (especialmente naquelas que lidam mais de perto com o digital) de "Regras de Responsabilidade Moral por Artefactos Computacionais[25]", onde os indivíduos seguem uma série de diretrizes sobre ética no uso e desenvolvimento de programas e outros ficheiros informáticos. Embora com diretrizes de caráter geral, é possível que estas influenciem e se tornem a base de futuros

[25] Tradução livre. No original, "Moral Responsibility for Computing Artifacts" é um documento criado no âmbito de um workshop realizado em 2010 nos EUA. Cf. (Stallings e Brown, 2018), *Computer Security – Principles and Practice*, 3ª edição, Pearson, United States of America

códigos de conduta sobre cibersegurança em vários países do mundo (Stallings e Brown, 2018).

3. ABORDAGEM METODOLÓGICA

3.1. Questão de partida e objetivos

Considerando que o marketing digital "(…) é a aplicação de estratégias de comunicação e marketing com vista à promoção/ marketing de produtos ou serviços através de canais digitais e de aparelhos eletrónicos" (Faustino, 2019: 21), e o facto de serem compostas por profissionais (marketeers) com fortes noções do funcionamento das redes sociais e do digital, bem como de o núcleo do seu negócio assentar nestes dois pontos, presume-se que tenham noções sólidas de comportamentos ciberseguros, de modo a protegerem a si e aos dados da empresa e dos clientes com quem trabalham diariamente. Tendo em consideração os pontos acima referidos, define-se como principal objetivo a realização de um estudo exploratório para a análise e compreensão sobre a forma como a comunicação sobre cibersegurança é realizada aquando da passagem para o teletrabalho em agências deste setor. "O estudo exploratório tem por objetivo conhecer a variável de estudo tal como se apresenta, seu significado e o contexto onde ela se insere" (Piovesan e Temporini, 1995: 321).

Com base neste objetivo e com o apoio da literatura existente sobre o tema, definiu-se enquanto pergunta de pesquisa "*Quais os impactos da pandemia de Covid-19 a nível da comunicação sobre cibersegurança em contexto de teletrabalho por agências de marketing digital?"* e como perguntas subsidiárias a) "*Quais as maiores dificuldades que um trabalhador enfrenta no desempenho de funções por teletrabalho*?", b) "*Os funcionários deste setor encontram-se bem informados sobre comportamentos ciberseguros em contexto de teletrabalho?"* e c) *"De que forma a comunicação sobre esta temática pode ser melhorada?"*

Para a obtenção das respostas pretendidas a estas perguntas optou-se pela realização de um estudo empírico que procurasse conhecer a opinião destes profissionais sobre esta temática, comparando com a literatura existente. O objetivo das entrevistas prende-se, principalmente, com a compreensão e reflexão sobre alguns dos desafios encontrados em teletrabalho, bem como quais as maiores falhas a nível da comunicação efetuada dentro destas agências, sobre cibersegurança.

3.2. Metodologia

3.2.1. Método

O método de análise escolhido para este estudo foi essencialmente qualitativo. Este método apresenta algumas desvantagens, como um número inferior de casos, bem como uma maior dificuldade na análise e interpretação dos dados recolhidos, devido à maior possibilidade de

recolher respostas diversificadas quando em comparação com outros métodos (Coutinho, 2011).

Contudo, tendo por base os objetivos pretendidos, revelou-se como o mais viável para a compreensão da posição dos entrevistados em relação ao tema, bem como para descrever experiências pelas quais estes passaram, graças à descoberta de significados "nas acções individuais e nas interacções sociais a partir da perspectiva dos actores intervenientes no processo" (Coutinho, 2011: 26). Esta abordagem de cariz indutivo permitiria, assim, criar comparações entre os dados recolhidos (Blaikie, 2000).

Devido à conjetura pandémica na altura da recolha dos dados, bem como à localização geográfica das agências, recorreu-se a entrevistas não presenciais, semiestruturadas, utilizando-se um guião previamente construído. Os critérios usados para a escolha deste método qualitativo de recolha dos dados prendem-se essencialmente com as caraterísticas enunciadas por Quivy e Campenhoudt (2005: 191-192): "Ao contrário do inquérito por questionário, os métodos de entrevista caracterizam-se por um contacto direto entre o investigador e os seus interlocutores (…)", permitindo assim aos entrevistados uma maior flexibilidade nas suas respostas, sem, no entanto, permitir uma excessiva abertura das mesmas, garantindo ao investigador a possibilidade de reencaminhar o entrevistado para os objetivos principais da entrevista caso este se afaste demasiado deles.

3.2.2. Definição da amostra

A constituição da amostra usada neste estudo teve natureza não probabilística sendo não-representativa da população em estudo: "A amostragem probabilística é aquela em que a seleção dos elementos da população para compor a amostra depende ao menos em parte do julgamento do pesquisador ou do entrevistador no campo" (Mattar, 2012: 125).

O e-mail foi a opção escolhida para efetuar os primeiros contactos com as empresas, bem como para explicar os objetivos do estudo. Mais tarde, alguns dos entrevistados preferiram ser contactados via *WhatsApp*, uma vez que nem sempre acediam com a mesma regularidade ao e-mail. Foram contactadas 59 agências a nível nacional, sendo que apenas 7 responderam. De entre essas agências, apenas 2 aceitaram participar sob as condições previamente acordadas no e-mail e reiteradas no momento da entrevista. Por esse motivo, não foi possível diversificar mais a amostra utilizada, tal como tinha sido inicialmente planeado.

3.2.3. Período em análise

Por ser um tema ligado ao funcionamento interno das organizações, optou-se pelo anonimato, quer dos participantes, quer das agências envolvidas, tendo os entrevistados concordado com

a referenciação nominal e alfabética usada neste estudo. Em função das limitações impostas pela atual crise pandémica, todas as entrevistas foram realizadas à distância, com recurso a ferramentas de videovigilância, sendo que o *Google Meet* foi a plataforma escolhida.

O período em análise na recolha de dados foi o decorrido entre março e setembro de 2020, uma vez que nele ocorreram vários momentos que serviram não só de mote e inspiração para o presente estudo, como ainda foram momentos cujo impacto influenciou os resultados da pesquisa efetuada, como o surgimento da pandemia de Coronavírus em Portugal, a primeira declaração do Estado de Emergência a nível nacional, e o posterior desconfinamento efetuado com o regresso a uma nova normalidade.

Assim, foram realizadas 5 entrevistas com o intuito de recolher opiniões sobre 5 esferas de análise:

1. Maiores desafios em teletrabalho;
2. Conhecimento sobre ciberameaças;
3. Formação sobre cibersegurança;
4. Falhas de cibersegurança em teletrabalho;
5. O papel do Estado e das próprias agências na proteção dos dados, pessoas e equipamentos.

Como se pretendia analisar estas esferas de um ponto de vista tanto do lado da administração, como do lado do funcionário, foram construídos previamente dois guiões, os quais diferem ligeiramente nas perguntas realizadas, consoante o cargo exercido pelo entrevistado (ver Anexos B e C).

A análise do conteúdo destas entrevistas tem como função “avaliar de forma sistemática um corpo de texto (…) por forma a desvendar e quantificar a ocorrência de palavras/ frases/ temas considerados “chave” que possibilitem uma comparação posterior” (Coutinho, 2011: 193).

4. ANÁLISE DAS ENTREVISTAS E DISCUSSÃO DE RESULTADOS

A amostra usada neste estudo é composta por 5 indivíduos do sexo masculino. A média de anos de experiência dos entrevistados no setor do marketing é de 9 anos. O tempo médio em que os entrevistados se encontram ao serviço das agências envolvidas no estudo é de 7 anos (ver Anexo A – Quadro II). Foram analisadas 2 agências de marketing digital, localizadas em Portugal Continental, e cujos escritórios se encontram, mais especificamente, no Porto e em Lisboa (ver Anexo A – Quadro I).

Para melhor desenvolver uma análise dos dados recolhidos, bem como uma formulação mais direta e objetiva dos resultados alcançados, optou-se pela divisão dos mesmos segundo os cinco pontos acima indicados e cujo desenvolvimento se seguirá ao longo das próximas páginas.

4.1. Maiores desafios em teletrabalho

Três dos entrevistados afirmaram que a maior dificuldade sentida durante o teletrabalho foi a ausência de contacto físico com os colegas, o que se refletiu numa posterior preocupação com o desenvolvimento de laços:

> A desintegração das relações interpessoais no trabalho. Esse é o maior desafio de todos. Porque há esta separação das pessoas não conviverem diariamente, terem de recorrer a uma câmara e nem sempre estarem disponíveis. Em teletrabalho nós fazemos muito mais coisas que aquelas que fazemos no escritório e depois não desenvolvemos esta relação de equipa, de fortalecimento de laços. [Entrevista #3]

Uma das dificuldades manifestadas prende-se com a organização das equipas e controlo do trabalho desenvolvido por cada membro bem como o desgaste emocional provocado pela dificuldade em separar o trabalho, da família e do lazer.

Um dos entrevistados declarou ainda que, embora o teletrabalho pudesse ser visto como algo negativo, principalmente devido ao isolamento sentido quando em comparação com o trabalho desenvolvido no escritório, estar em casa permitiu-lhe um aumento da produtividade:

> Agora, a nível de produtividade, gestão do trabalho, cumprimento de *timings*, diria que o teletrabalho é muito superior em comparação com estar no escritório. Porque apesar de tudo, tu estás mais focado na tua *timeline* e no tempo que tens de dedicar a cada projeto e, por norma, neste último ano e meio, as coisas têm corrido de forma mais fluída, precisamente porque não tens tantas interrupções. Assim consegues responder mais rápido e melhor, ou seja, dar mais de ti ao projeto. [Entrevista #2]

Os entrevistados de ambas as agências referiram que não existiram problemas com o desenvolvimento e a entrega de projetos, principalmente porque, trabalhando no digital, conseguem adaptar-se relativamente bem e com maior rapidez ao teletrabalho, algo que nem sempre é possível em outros setores.

Também a comunicação com outros elementos da equipa não foi afetada pelo trabalho: em ambas as agências os entrevistados referiram que a nível de comunicação não houve problemas, precisamente porque sendo agências que trabalham com o digital, existe uma certa preparação para este tipo de situações. No entanto, um dos entrevistados acredita que a riqueza dos trabalhos acabou por ser prejudicada:

> Nós, sendo uma equipa digital, claro que temos uma série de ferramentas (Trello, ferramentas de comunicação) que utilizamos e que nos permitem organizar e controlar o trabalho que cada um está a fazer e que nos permitiram uma boa adaptação a este cenário do teletrabalho. [Entrevista #5]

> Não tivemos nenhum atraso nos projetos porque a comunicação operacional à distância funciona lindamente e, portanto, fez-se. Agora se me disseres a riqueza dos trabalhos ou o enriquecimento individual das pessoas, esse foi muito menor. Mas não acho que a entrega em si tenha sido prejudicada pelo teletrabalho. [Entrevista #1]

Quando questionados sobre potenciais dificuldades por parte dos funcionários para desempenharem as suas funções por esta via, apenas foi indicado pelos colaboradores de uma das agências a necessidade de reformular os seus contratos com as respetivas operadoras de telecomunicações, de forma a terem uma ligação à Internet que lhes permitisse trabalhar melhor. Nas duas agências foi indicado apoiar os colaboradores em eventuais despesas resultantes destas alterações.

4.2. Conhecimentos sobre ciberameaças

Neste ponto pretende-se avaliar os conhecimentos dos entrevistados sobre o significado de ciberameaça e quais aquelas que consideram mais perigosas, colocando em risco não só os dados pessoais como ainda os dados da própria agência e clientes.

No geral, todos os entrevistados manifestaram bons conhecimentos teóricos do que é uma ciberameaça e dos impactos da mesma nos sistemas das agências e na vida pessoal e profissional das vítimas. O *phishing* foi o exemplo mais referido por três dos entrevistados, embora afirmem existir alguma facilidade para reconhecer esse tipo específico de ciberataque:

> Eu tenho alguma cultura, conhecimento, leio algumas coisas, tenho pessoas ligadas a departamentos de segurança noutras empresas e sei quais são os ataques e aquilo que mais me "choca" é a desinformação de algumas pessoas não perceberem como é fácil perceber que um e-mail é *phishing*. [Entrevista #3]

Por outro lado, para dois dos entrevistados os ataques por *ransomware* mostraram-se particularmente perigosos, sendo essa a sua principal preocupação quando se fala de ciberameaças:

> Uma ciberameaça nesta altura é sobretudo o resgate dos nossos dados por terceiros, através de uma técnica chamada *ransomware*. Então nesta altura, quando se fala em cibersegurança, o primeiro pensamento vai logo para aí: para o *ransomware*, para o pedido de resgate, que pode ir para milhares de euros. Portanto isto de facto é uma preocupação. [Entrevista #4]

Embora com preocupações distintas em relação às ciberameaças, as duas agências não demonstraram um receio extremo perante as mesmas, possivelmente por ciberataques não serem tão comuns dentro deste setor, o que as leva a não investir demasiado tempo e recursos nessa matéria, embora nunca deixem de reconhecer a importância da mesma.

4.3. Formação sobre cibersegurança

Nesta esfera procurou avaliar-se de que forma é realizada a comunicação sobre cibersegurança dentro da agência e se estas dispõem de mecanismos que visem aumentar o conhecimento dos seus funcionários sobre esta temática. Procurou-se ainda recolher algumas opiniões sobre a importância da formação sobre cibersegurança e o que isso mudaria a nível do desenvolvimento dos projetos.

Os entrevistados de uma das agências declararam não dar qualquer tipo de formação em cibersegurança, nem no momento da contratação dos funcionários nem no decurso do desempenho das suas funções. Contudo, reconhecem esse aspeto como um ponto para o qual deveria haver mais informações bem como o desenvolvimento de ações de modo a melhorar os conhecimentos, não só dos próprios funcionários como da população em geral:

> Acho que em Portugal ninguém, à exceção de engenheiros informáticos e mais algumas pessoas que trabalham dentro da área, tem capacidade para tal. Ou seja, no mundo em que vivemos atualmente, em que tudo é digital, acho que todos nós devemos ter uma

> ligeira formação em contexto de trabalho do que é que deveríamos fazer caso isso acontecesse. [Entrevista #2]

Por outro lado, o entrevistado da segunda agência referiu dar algumas instruções aos funcionários na altura em que estes começam a trabalhar, sendo que posteriormente essas indicações vão sendo relembradas pelo departamento de IT.

> Nós temos políticas de segurança que são implementadas desde o início e isto tem a ver com a entrada de funcionários, onde é fornecido equipamentos a cada um para trabalharem e são dadas instruções de todo o tipo de foros: utilização dos equipamentos, regras de boa conduta, segurança e cuidados a ter. [Entrevista #5]

Nas duas agências é reconhecida a importância de uma formação contínua e uma melhoria nesta temática, mesmo a nível interno. Em nenhuma delas se averigua, na altura da contratação dos funcionários, se estes possuem algum tipo de conhecimentos ou boas práticas de cibersegurança, confiando nos princípios éticos individuais de cada colaborador.

> Nós não verificamos, pelo menos proactivamente. Normalmente só atuamos sobre um problema. Partimos do princípio que as pessoas têm a sua própria ética e sabem o que fazer e não fazer em relação à cibersegurança. [Entrevista #1]

Questionados sobre o papel da formação em cibersegurança, um dos entrevistados referiu que um conhecimento mais sólido sobre o assunto poderia ajudar os utilizadores a trabalharem de forma mais confortável, pois saberiam o que fazer em caso de ameaça ao sistema:

> Acho que deveria ser implementado algum processo nas empresas (e cada uma decidiria qual seria esse processo), para formar as pessoas e dar-lhes as ferramentas para saber o que fazer quando acontece um ciberataque. Claro que tem que haver um procedimento porque tu estás numa empresa, estás a fazer o teu trabalho e de repente há um ciberataque: O que é que tu fazes? Qual é a tua primeira reação? Quais são os procedimentos a tomar? A quem devo reportar? [Entrevista #2]

Embora não pareça ser reconhecida uma necessidade imediata para a criação e melhoria a nível da comunicação sobre cibersegurança, a necessidade de formação foi um dos pontos onde os entrevistados mais concordaram, demonstrando abertura para possíveis sugestões e avanços nesse sentido.

4.4. Falhas de cibersegurança em teletrabalho

Neste ponto o objetivo foi analisar se existiram ciberataques no período de tempo em análise, bem como a opinião dos entrevistados sobre aquelas que consideravam ser as maiores causas para o aumento das fragilidades em cibersegurança. As duas agências indicaram não terem sofrido ciberataques em teletrabalho, embora reconheçam algumas tentativas ocorridas:

> Tentativas sim, sobretudo dentro do grupo de *brute force*[26]. Mas nunca houve por uma razão: nós utilizámos como comunicação VPNs com dupla encriptação. [Entrevista #4]

Um dos entrevistados indicou que as maiores falhas de cibersegurança quando em teletrabalho estavam muito relacionadas com aquilo que cada colaborador tinha no seu lar:

> Acho que tem muito a ver com aquilo que cada um tem em casa: tipo de acesso, se o equipamento é mais moderno ou mais antigo… [Entrevista #5]

Foi ainda referido por dois entrevistados que a distração e o desconhecimento desempenham papéis fundamentais no aumento da possibilidade de sofrer um ciberataque:

> Tirando um caso ou outro, que não têm a noção do que é uma rede empresarial e acham que o computador da empresa é o computador pessoal e às vezes não conseguem fazer essa ligação, e esquecem-se que estão a comprometer a companhia toda. Mas isso é raro acontecer e, quando acontece é por desconhecimento. [Entrevista #4]

> Portanto, e-mails que tenham determinadas caraterísticas é fácil percebermos que são para ignorar, mas há colaboradores que, mesmo assim, tendem a seguir os passos que lhes pedem e que comprometem a segurança. […] Sinto que essa desinformação que me parece ser relativamente acessível, principalmente quando estamos a falar de faixas etárias bastante jovens, […] já não devia ser um problema, até porque somos constantemente bombardeados com essas informações mesmo na televisão. [Entrevista #3]

Embora tenham referido que não houve registo de acidentes de cibersegurança em contexto de teletrabalho, essa informação foi salientada sob a forma “de que tenha registo”, desconhecendo-se se, de facto, existiram ciberataques que não tenham sido reportados.

[26] Método através do qual o atacante usa todas as combinações possíveis para encontrar a senha de acesso aos sistemas. Fonte: https://csrc.nist.gov/glossary/term/brute_force_password_attack

Salienta-se ainda que todos os entrevistados referiram o fator humano como uma das principais causas para falhas de cibersegurança.

4.5. O papel do Estado e das agências

O último ponto em análise diz respeito ao conhecimento dos entrevistados em matéria legislativa e o que poderia ser alterado tanto da parte do Estado como das próprias empresas. Os entrevistados afirmaram não possuir grandes conhecimentos sobre a ação do Estado no papel da cibersegurança. Todos referiram que a cibersegurança é importante, não só em contexto de teletrabalho como pessoal, mas manifestaram alguma incerteza sobre o papel do Estado na regulamentação e fiscalização sobre esta temática:

> Confesso que não tenho grandes conhecimentos para te conseguir responder a isso. Tenho muitas dúvidas relacionadas com uma presença mais forte do Estado em áreas muito relacionadas com a privacidade das pessoas e empresas. [Entrevista #5]

> O Estado tem de colocar ao seu alcance todos os meios para prevenir e atuar sobre isto, mas eu não sei, tecnicamente, até onde é que o Estado pode ir, pois a fiscalização sobre cibersegurança para mim ainda é um pouco difícil de perceber. [Entrevista #1]

Uma das preocupações mais frequentemente apresentada foi o papel da privacidade e vigilância online o que leva os entrevistados a indicar que o Estado não deveria interferir nas políticas de cibersegurança já existentes:

> Não porque se calhar depois também iria interferir com a privacidade das pessoas. […] Eu acho que o princípio da Internet é circularmos com liberdade. Há aqui o risco de, ao regulamentar tudo muitíssimo bem e um dia destes tu não podes aceder a um determinado conteúdo porque o Estado te diz que já acedeste a ele vezes demais, ou pior ainda. [Entrevista #4]

Como solução, a generalidade dos entrevistados indicou que devem ser as próprias agências a implementar as suas próprias normas e regras de conduta sobre cibersegurança, ficando ao critério de cada uma delas quais os procedimentos a tomar em caso de ciberataque:

> É importante, sem dúvida, mas acho que o Governo nunca vai investir nisso e a solução passa por partir das próprias agências, porque no país em que vivemos o setor privado é muito alheio a tudo o resto, é muito deixado de lado e podes ver isso noutras situações. Por isso, acho que cada empresa é que deve implementar o seu método. [Entrevista #2]

Os entrevistados reconhecem, assim, a importância do Estado em matéria legislativa; contudo, não demonstram demasiado interesse em qualquer alteração às leis existentes sobre cibersegurança, preferindo restringir essa informação para os círculos internos de cada agência, sendo cada uma responsável pela formação e atuação nesse sentido.

5. CONSIDERAÇÕES FINAIS

O estudo exploratório que aqui se apresenta partiu de uma revisão literária sobre o impacto do digital na sociedade, a cibersegurança e legislação existente, usada como fundamento para uma análise de conteúdo baseada nos dados recolhidos em entrevistas realizadas a membros da Administração e colaboradores de agências de marketing digital portuguesas.

Em primeiro lugar, em relação à pergunta de partida, conclui-se que a atual pandemia de Covid-19 não teve impactos significativos a nível da comunicação sobre cibersegurança em contexto de teletrabalho. A principal causa para isto diz respeito à preparação das próprias agências para o teletrabalho: ao contrário do que aconteceu com outros setores da indústria, o setor do marketing digital, pelas suas caraterísticas adaptou-se sem problemas relevantes, não sendo o teletrabalho mais do que aquilo que já desenvolviam nos escritórios.

Ainda assim, em relação à pergunta subsidiária a), os dados recolhidos indicam que o desempenho laboral dos cinco entrevistados não foi isento de pontos negativos, estando o isolamento social no topo dos mesmos. Foi ainda referida uma preocupação inicial com o foco dos funcionários quando em casa, o qual poderia impactar negativamente os projetos em curso, durante o primeiro mês em teletrabalho. Outro ponto salientado diz respeito ao aumento da carga laboral, embora não tenha sido possível aferir se esse aumento foi sentido por todos os indivíduos. Portanto, as maiores dificuldades apresentadas por estes colaboradores foram: isolamento social, preocupação com a sua prestação laboral e aumento da carga de trabalhos a desenvolver.

Na pergunta subsidiária b), conclui-se que os membros deste setor se encontram bem informados sobre comportamentos ciberseguros, tanto em contexto de teletrabalho como no escritório. Mais uma vez, o facto de trabalharem diariamente com o digital e dados dos clientes demonstra não só alguma preparação como ainda alguma confiança nas ações desenvolvidas pelos utilizadores no digital. No entanto, os entrevistados admitem não se encontrarem informados o suficiente sobre todas as atitudes e procedimentos a tomar tanto para prevenir como para resolver um ciberataque, motivo pelo qual indicam por unanimidade a necessidade de rever as políticas internas das agências e reformular alguma da comunicação realizada. Assim, encontra-se como resposta à pergunta subsidiária c), o investimento em formações internas e *reminders* constantes sobre regras a respeitar em matéria de cibersegurança.

Embora não vá de encontro a nenhuma pergunta formulada na metodologia, conclui-se ainda que embora não exista um conhecimento elevado sobre as políticas desenvolvidas pelo Estado, os entrevistados demonstraram uma preocupação com a interferência das políticas de cibersegurança na sua privacidade, receando uma vigilância e controlo apertado do Estado sobre as suas ações desenvolvidas online.

Para futuros trabalhos sobre esta temática sugere-se a utilização de um método de análise quantitativo, por exemplo, através de um questionário para que seja possível uma maior recolha e variedade de dados. Sugere-se ainda uma possível comparação do cenário português com o cenário internacional nesta matéria

REFERÊNCIAS BIBLIOGRÁFICAS

Abass, Islam Abdalla Mohamed (2018), "Social Engineering Threat and Defense: A Literature Survey" *Journal of Information Security,* (9), pp.257-264.

Andrade, Priscila (2013), *«Quem vigia o vigilante?» Entre a Vigilância e a Privacidade na Sociedade em Rede*, Dissertação de Mestrado em Comunicação, Cultura e Tecnologias da Informação, Departamento de Sociologia, Iscte – Instituto Universitário de Lisboa.

Antunes, Mário e Baltazar Rodrigues (2018), *Introdução à Cibersegurança: A Internet, os Aspetos Legais e a Análise Digital Forense*, 1ª ed., FCA – Editora de Informática, Lisboa.

Atzori, L., Antonio Iera e Giacomo Morabito (2016), "Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm", *Ad Hoc Networks*, 56.

Baptista, Isabel Margarida Afonso da Silva (2017), *O Fator Humano na Cibersegurança*, Dissertação de Mestrado em Segurança da Informação e Direito no Ciberespaço, Instituto Superior Técnico – Lisboa.

BBC (2010), "Four in five regard internet access as fundamental right: global poll" *Press Office* (online). Consultado em: 14.11.2020. Disponível em: http://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03_march/07/poll.shtml

Bell, Daniel (1973), *The Coming of Post-Industrial Society – Venture in Social Forecast*, Basic Books, New York

Belzunegui-Eraso, Angel e Amaya Erro-Garcés (2020), "Teleworking in the Context of the Covid-19 Crisis" *Sustainability* 12 (May).

Blaikie, Norman (2000), *Designing Social Research*, Polity Press, Cambridge.

Boehm, Katharina et. al. (2020), "Telemedicine Online Visits in Urology During the COVID-19 Pandemic: Potential, Risk Factors and Patients Perspective" *European Urology* (April).

Castells, Manuel e Gustavo Cardoso (2006), *A Sociedade em Rede – Do Conhecimento à Acção Política,* Imprensa Nacional – Casa da Moeda.

Centro Nacional de Cibersegurança (2019), *Quadro Nacional de Referência para a Cibersegurança*. Consultado em: 13.06.2021. Disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

Centro Nacional de Cibersegurança (2020a), *Boletim Observatório de Cibersegurança* 2 (maio). Consultado em: 13.11.2020. Disponível em: https://www.cncs.gov.pt/content/files/boletim_observatorio_maio2020.pdf

Centro Nacional de Cibersegurança (2020b), *Alerta COVID-19 e as ciberameaças* (online). Consultado em 30.04.2021. Disponível em: https://www.cncs.gov.pt/recursos/noticias/alerta-covid-19-e-as-ciberameacas/

Centro Nacional de Cibersegurança (2020c), *Relatório Cibersegurança em Portugal: Ética e Direito* (online). Consultado em 05.05.2021. Disponível em:

https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriocibersegurança_cncs.pdf

Centro Nacional de Cibersegurança (2020d), *Relatório Cibersegurança em Portugal: Riscos e Conflitos* (online). Consultado em 05.05.2021. Disponível em: https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriocibersegurança_cncs.pdf

Centro Nacional de Cibersegurança (2021), *Relatório Cibersegurança em Portugal: Riscos e Conflitos* (online). Consultado em 02.06.2021. Disponível em: https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2021__observatoriocibersegurança_cncs.pdf

Comissão Nacional de Proteção de Dados (2020), *Orientações sobre o controlo à distância em regime de teletrabalho* (online). Consultado em 11.09.2021. Disponível em: https://www.cnpd.pt/media/zkhkxlpx/orientacoes_controlo_a_distancia_em_regime_de_teletrabalho.pdf

Coutinho, Clara Pereira (2011), *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática*, Grupo Almedina, Coimbra.

Dal Bello, Cíntia (2011), "Visibilidade, Vigilância, Identidade e Indexação: a questão da privacidade nas redes sociais digitais" *O Estatuto da Cibercultura no Brasil* 34 (1), 1º semestre, LOGOS 34.

Deleuze, Gilles (2008), *Conversações*, São Paulo (7ª reimpressão) trad. Peter Pál Pelbart, (Edição original, 1992) Editora 34.

Espanha, Rita e Tiago Estêvão (2017), "A Vigilância Lateral e Participativa na Web 2.0" *Sociologia*, (Online) 33, pp.115-133. Disponível em uma Base de dados: Scielo.

Estêvão, Tiago Manuel Vaz Pinheiro (2014), *A Vigilância nas Sociedades Contemporâneas – O Estudo de Caso do INDECT*, Dissertação de Mestrado em Comunicação, Cultura e Tecnologias da Informação, Departamento de Sociologia, Iscte – Instituto Universitário de Lisboa.

Fairweather, N. Ben (1999), "Surveillance in Employment: The Case of Teleworking" *Journal of Business Ethics* 22 (1), pp. 39-49, October.

Faustino, Paulo (2019), *Marketing Digital na Prática*, 1ª edição, Marcador, Lisboa.

Foucault, Michel (1999), *Vigiar e Punir: nascimento da prisão*, (20ª edição) trad. Raquel Ramalhete, (Edição original, 1987), Vozes, Petrópolis.

Fuchs, Christian (2008), *Internet and Society: Social Theroy in the Information Age*, Routledge, New York

Fuchs, Christian (2010), "Social networking in the surveillance society" *Ethics and Information Technology*, vol. 12. pp. 171-185, June.

Fuchs, Christian (2011), “New Media, Web 2.0 and Surveillance” *Sociology Compass* vol.5, pp.134-147

Georgiadou, Anna, Spiros Mouzakitis e Dimitris Askounis (2021), “Working from home during COVID-19 crisis: a cyber security assessment survey” *Security Journal* (2021).

Hadnagy, Christopher (2011), *Social Engineering – The Art of Human Hacking* Wiley Publishing, Inc., Indianapolis, Indiana.

Hootsuite (2020), *We Are Social* (online). Consultado em 23.11.2020. Disponível em: https://wearesocial.com/digital-2020

International Labour Organization (2020), *Teleworking during the COVID-19 pandemic and beyond – A Practical Guide* (online). Consultado em 4.05.2021. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/instructionalmaterial/wcms_751232.pdf

INE (2020), *Working from home – Labour Force Survey ad hoc module 2nd quarter of 2020*, Press Release, 5th August. Disponível em: https://ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=445841978&DESTAQUESmodo=2

Kokolakis, Spyros (2017), “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon” *Computer and Security* vol. 64, pp.122-134

Lipson, Howard F. (2002), “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues” *Networked Systems Survivability Program,* November, Pittsburgh.

Lyon, David (1998), “The World Wide Web of Surveillance: The Internet and Off-World Power” *Flows, Information, Communication & Society* vol. 1, pp. 91-105, citado por Estêvão, Tiago Manuel Vaz Pinheiro (2014), *A Vigilância nas Sociedades Contemporâneas – O Estudo de Caso do INDECT*, Dissertação de Mestrado em Comunicação, Cultura e Tecnologias da Informação, Departamento de Sociologia, Iscte – Instituto Universitário de Lisboa.

Lyon, David (2018), *The Culture of Surveillance: Watching as a Way of Life*, Polity Press, Cambridge

Malecki, Florian (2020), “Overcoming the security risks of remote working” *Computer Fraud & Security* vol. 2020, issue 7, pp. 10-12.

Manokha, Ivan (2020), “Covid-19: Teleworking, Surveillance and 24/7 Work. Somo Reflexions on the Expected Growth of Remote Work After the Pandemic” *Political Anthropological Research on International Social Sciences* 1, pp. 273-287.

Matos, Pedro Carvalhais de Abreu (2018), *Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas*, Dissertação de Mestrado em Economia e Políticas Públicas, Departamento de Economia Política, Iscte – Instituto Universitário de Lisboa.

Mattar, Fauze Najib (2012), *Pesquisa de Marketing- Edição Compacta*, 5ª ed. Elsevier Editora, Brasil.

Mendes, Diogo Carvalho (2014), *Técnicas de Hacking para Anonimização na Internet*, Dissertação de Mestrado em Segurança de Sistemas de Informação, Universidade Católica Portuguesa.

Michaelides, Nadine (2020), "Remote working and cyber security literature review" *Psychological Contract and Cyber Psychology in Information and Cyber Security*.

Patel, K. *et. al.* (2016), "Internet of Things – IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges" *International Journal of Engineering Science and Computing* (Online), 6 (5). Consultado em: 25.11.2020. Disponível em uma Base de dados: Research Gate.

Payton, Theresa M & Theodore Claypoole (2014), *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family,* 1ª edição, Rowman & Littlefield, United Kingdom.

Pedro, Filipa Alexandra Rodrigues (2014), *A Privacidade no Local de Trabalho – A admissibilidade dos meios de vigilância como meios de prova* Dissertação de Mestrado em Direito das Empresas, Departamento de Economia Política, Iscte- Instituto Universitário de Lisboa.

Piovesan, Armando e Edméa Rita Temporini (1995), "Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública" *Revista Saúde Pública*, 29 (4), pp. 318-325.

Pranggono, Bernardi e Abdullahi Arabo (2020), "COVID-19 pandemic cybersecurity issues" *Internet Technology Letters,* vol. 4, issue 2.

Quaglio, Gianluca e Sophie Millar (2020), "Potentially negative effects of internet use" *Scientific Foresight Unit (STOA) – European Parliamentary Research Service* (online). Consultado em 30.09.2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641540/EPRS_IDA(2020)641540_EN.pdf

Quivy, Raymond & Luc Van Campenhoudt (2005), *Manual de Investigação em Ciências Sociais*, 4ª edição, Gradiva, Lisboa.

Rosa, Fábio Medeiros da e Leandro Chevitarese (2017), "Vigilância e relações de poder nas redes sociais: questões éticas na sociedade contemporânea" *Organicom* 14 (27).

Rossoni, Caroline e Iuri Bolesina (2014), "A Teoria dos Círculos Concêntricos e a Proteção à Vida Privada: Análise ao Caso Von Hannover vs. Alemanha, Julgado pela Corte Europeia de Direitos Humanos" *XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea – VII Mostra de Trabalhos Jurídicos Científicos*

Soares, Herbert; Nelcileno Araújo e Patrícia Souza (2020), “Privacidade e Segurança Digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade” *Conference: Workshop on the Implications of Computing in Society*, Cuiabá.

Stallings, William e Lawrie Brown (2014), *Computer Security – Principles and Practice*, 3ª edição, Pearson, United States of America

Trappe, Wade e Jeremy Straub (2018), “Journal of Cybersecurity and Privacy: A New Open Acess Journal” *Journal of Cybersecurity and Privacy*, 1 (June)

Trepte, Sabine (2015), “Social Media, Privacy and Self-Disclosure: The Turbulence Caused by Social Media’s Affordances” *Journal of Social Media + Society*, 1 (May)

Tully, S. (2014). “A Human Right to Access the Internet? Problems and Prospects” *Human Rights Law Review* 14 (1-21)

Van Djick, Jose; Thomas Poell & Martijn De Waal (2018), *The Plataform Society: Public Values in a Connective World*, Oxford Press University, United States of America

Wang, Lidong e Cheryl Ann Alexander (2021), “Cyber security during the COVID-19 pandemic” *AIMS Eletronics and Electrical Engineering*, vol. 5, issue 2, pp. 146-157

Weber, Rolf H. e Evelyne Studer (2016), “Cybersecurity in the Internet of Things: Legal aspects” *Computer Law & Security Review* 32, pp. 715-728

Webster, Frank (1995), *Theories of the Information Society*, Routledge, London and New York

Wen Gong, Z., Li Rodney e L. Stump (2007), “Global internet use and access: cultural considerations” *Asia Pacific Journal of Marketing and Logistics*, 19, pp. 57-74

FONTES

Lei n.º 7 de 2009, *Diário da República n.º 30/2009, Série I de 2009-02-12*, Código do Trabalho

Lei nº 109 de 2009, *Diário da República nº 179/2009, Série I de 2009-09-15*

Relatório Anual de Segurança Interna (2020), *Sistema de Segurança Interna*.

Regulamento (EU) 2019/ 881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019

Resolução do Conselho de Ministros nº 92 de 2019, *Diário da República nº 108/2019, Série I de 2019-06-05,* pp. 2888-2895

ANEXOS

ANEXO A – CARATERIZAÇÃO DAS ENTREVISTAS

TEMA: Comunicação sobre cibersegurança em agências de marketing digital em contexto de teletrabalho.

OBJETIVO GERAL: Analisar e compreender possíveis semelhanças e diferenças nos processos comunicativos sobre a cibersegurança em teletrabalho, entre as agências analisadas e a literatura existente.

QUADRO I – Caraterização das agências envolvidas

AGÊNCIA	ZONA	DATA DA CRIAÇÃO	TAMANHO*
A	Porto	2009	11-50 funcionários
B	Lisboa	2009	11-50 funcionários

Nota: As agências visadas consentiram a identificação por referência alfabética.

*Segundo dados do LinkedIn

QUADRO II – Caraterização da amostra dos funcionários entrevistados

ENTREVISTA	AGÊNCIA	CARGO	TEMPO DE EXPERIÊNCIA NA ÁREA	TEMPO AO SERVIÇO DA AGÊNCIA
#1	A	Fundador e Proprietário	12 anos	12 anos
#2	A	Designer	9 anos	6 anos
#3	A	*Head of Business*	6 anos	18 meses
#4	B	Técnico de IT	N/A	11 anos
#5	B	*CEO*	10 anos	4 anos

QUADRO III – Caraterização das entrevistas realizadas

ENTREVISTA	DATA	DURAÇÃO	SUPORTE
#1	07/ 10/ 2021	00:12:46	Google Meet
#2	08/10/ 2021	00:23:36	Google Meet
#3	12/10/ 2021	00:18:49	Google Meet
#4	12/10/2021	00:16:50	Google Meet
#5	12/10/2021	00:13:15	Google Meet

ANEXO B – GUIÃO DA ENTREVISTA À ADMINISTRAÇÃO E TÉCNICO DE IT

Enquadramento prévio: Explicação dos objetivos do estudo, funcionamento da entrevista, anonimato e permissão para gravar a entrevista para posterior transcrição e análise.

1. Há quanto tempo trabalha no setor do Marketing Digital?
2. Há quanto tempo trabalha nesta agência?
3. Na sua opinião, quais os maiores desafios colocados na passagem para o teletrabalho?
4. O que entende por ciberameaça?
5. Existe algum tipo de cultura de cibersegurança dentro da agência?
6. Verificam se os funcionários têm conhecimento das normas e boas práticas de cibersegurança, tanto na altura da sua contratação como ao longo da sua jornada laboral?
7. Proporcionam algum tipo de formação sobre este tema?
8. Houve alguma atenção especial na comunicação ou alteração das boas práticas de cibersegurança devido à pandemia?
9. Quais os principais problemas registados em relação à cibersegurança em contexto de teletrabalho?
10. Quais considera serem as maiores falhas a nível da cibersegurança em teletrabalho?
11. Registaram-se mais queixas de ciberataques durante a pandemia?
12. Acha que o Estado deveria investir mais na regulamentação e fiscalização da cibersegurança?

ANEXO C – GUIÃO DA ENTREVISTA AOS COLABORADORES

Enquadramento prévio: Explicação dos objetivos do estudo, funcionamento da entrevista, anonimato e permissão para gravar a entrevista para posterior transcrição e análise.

1. Há quanto tempo trabalha no setor do marketing digital?
2. Há quanto tempo trabalha nesta agência?
3. No decorrer do teletrabalho, quais foram as principais dificuldades sentidas?
4. Sabe o que é uma ciberameaça?
5. Sentiu alguma dificuldade ou falta de apoio na resolução de uma ciberameaça?
6. Conhece os procedimentos da agência em caso desta sofrer um ciberataque?
7. De que forma a presente pandemia de Covid-19 impactou a sua prestação em teletrabalho e a comunicação entre colaboradores e agência?
8. Na sua opinião, o que poderia ser feito para melhorar a comunicação e os procedimentos a seguir de modo a prevenir um ciberataque?
9. Acha que o Estado deveria investir mais na fiscalização e regulamentação da cibersegurança?