CYBERLAW

by CIJIC

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

CYBERLAW by CIJIC

EDIÇÃO N.º XI – MARÇO DE 2021

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Finda Março do ano de 2021.

Passou um ano desde que o mundo se confinou, massivamente. Fechados, em casa, nunca como a partir disto o acesso à *Internet* se nos desvelou como um direito humano fundamental.

O sonho de uma *internet* livre, neutral, aberta, inclusiva, universal será possível?

Provavelmente muitos de nós, que navegam por ela, num ou noutro canto de conversação e/ou *stop by* possível a partir de um dos nossos hodiernos cárceres físicos, já nos deparámos com um curioso grafo. Nele consta uma espécie de sondagem onde à pergunta: *"Quem fez mais pela digitalização da sua organização no último ano?"*, a percentagem do vencedor surpreende.

Não, não foi o CEO da organização. Também não, não foi o CISO (quando as organizações os têm). Sim, também não foi nenhum diretor de nenhum departamento da organização.

O principal responsável, sim, foi ela: a pandemia de covid-19.

É inegável. A pandemia acelerou o processo de digitalização de grande parte das interações humanas, sejam elas de qualquer natureza, escola, comércio, socialização.

Não obstante, por mais benefícios que este *input*, à *força bruta*, tenha trazido, a humanidade tem ainda um caminho muito longo para percorrer.

Num plano macro, que convoca a humanidade, combater ferozmente a exclusão digital, com particular enfoque nos reversos, *i.e.*, mais novos e mais velhos; sociedades desenvolvidas/mais pobres.

E se o acesso não é universal (sê-lo-á algum dia?), plural, em condições idênticas, inclusivo…também não deixará de ser preocupante, dentro daqueles que podem aceder, o número de indivíduos com falta de formação, com falta de um mínimo de educação/formação para usufruir da Rede.

Atente-se, porém, num plano micro, por exemplo, no caso português.

Entregue, neste último dia de Março de 2021, o RASI2020[1], nele despontam algumas evidências sobre a temática da falta de educação para o *ciber*. Os crimes praticados na e pela *Internet*, nomeadamente, *phishing*, *vishing*, *ransomware* e extorsão[2], em passo crescente, decorrem de variadas falhas ao nível do utilizador. Sobressai, da leitura crua dos números, uma inexistente cultura de ciberhigiene. A facilidade de promoção de engenharias sociais avulsas. É esta omissão de cibereducação responsável pela inabilidade em detetar o logro e burlões, em actividade fervorosa. No compasso da oferta/procura de produtos através do digital, se as trocas aumentam exponencialmente, paralela e em acompanhamento, as situações de fraude, burla, roubo, *Money mules*, etc., *idem*.

As múltiplas deficiências ao nível do utilizador – o famoso factor humano é implacável - e a violência de uma *digitalização à força bruta* de uma grande maioria das organizações, combinadas… dão razão de ser à *tame joke* informática de que, *na prática, em termos de ataques e crimes informáticos, só há dois tipos de organizações: as que sabem que já foram atacadas e as que ainda não o sabem* (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

1 Disponível para consulta em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d (último acesso 31MAR21)
2 *Vide* páginas 67 e ss do RASI2020.

Torna-se inadiável que, paralelamente ao percurso do Direito no séquito da acelerada digitalização, as organizações, as pessoas, o Estado, entendam, decisiva e finalmente, a importância da segurança da informação[3].

Apaticamente, e em crise, as omissões perduram. Sedimentam.

Os alertas não chegam a bom porto. Provenham eles de serviços mais ou menos capacitados do Estado, sejam serviços secretos nacionais, sistema de segurança interna, observatórios…jaz, apenas, a constatação impotente de que "(…) *observa-se um aumento da espionagem através de ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado. Uma das consequências da sofisticação enunciada, prende-se com a crescente dificuldade em destrinçar ataques informáticos para efeitos de crime económico ou de crimes de sabotagem, dirigidos a empresas e grupos de empresas com relevância no tecido empresarial nacional*."

No presente, de crescente digitalização, de cascata informacional, já todos sabemos que não é a quantidade de informação que serve à melhor tomada de decisão; é a qualidade. Mostra-se-nos angustiante o sublinhado de "*ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado"*.

O Estado, como nunca, até como condição de promoção e prossecução geracional, tem o dever de defender um desígnio de soberania consubstanciado, precisamente, na superioridade informacional.

Conhecerá o Estado a capital importância da superioridade informacional?

Estará capacitado, humana e tecnologicamente, para proteger, o mais eficazmente possível, os seus mais valiosos *assets*, as suas infraestruturas mais críticas?

Severa, a frieza dos parágrafos, no contexto pandémico Covid-19: "*No que concerne a outra das ameaças, i.e., as operações cibernéticas ofensivas, foram*

3 Ainda, no RASI2020 agora dado a conhecer, «(…) *No universo da ciberespionagem, registaram-se novos ciberataques contra infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico."*», página 102.

identificados agentes estatais e não estatais, visando entidades públicas e privadas, em particular no que respeitou à exploração de oportunidades…Verificaram-se inúmeros ciberataques registados contra instituições do setor da saúde, bem como operações de ciberespionagem contra entidades de investigação cientifica, particularmente envolvidas na pesquisa de terapêuticas e de vacinas contra a doença em apreço."

A segurança da informação, e a superioridade informacional que daí possa erigir, são, no contexto, de suma importância.

Infelizmente, as ameaças são múltiplas. Se, como veremos nesta nova edição, a Segurança da informação nas organizações(SiO) é tema fulcral, a erosão, de direitos fundamentais humanos, não descola de uma objetificação pronunciada da pessoa, do ser individual. Discreta, mas de forma expedita, as *oportunidades geradas pelo contexto pandémico*, têm servido para que o Estado arroje sistemas de videovigilância por múltiplas localidades nacionais[4]. A febre dos sistemas *CCTV* públicos segue a passo acelerado.

Em simultâneo, embora a aplicação *stayawaycovid* não tenha vingado, ainda, é certo que o controlo à distância da pessoa irá figurar, brevemente, em alguma medida legislativa. Notemos, ainda no contexto da pandemia, por exemplo, e em pleno estado de emergência, os níveis de mobilidade do cidadão. Com a proibição de circulação fora-do-concelho e a aproximação do tema festivo pascal, na semana de 25/26 de Março, acordámos com a notícia: "*Portugueses fogem para longe das restrições: um em cada dez dormiu a mais de 100 quilómetros de casa esta quinta-feira.*"[5].

A observação - próxima da realidade? - feita por uma consultora privada[6], revelando que mais de *um milhão de portugueses dormiu fora de casa*, curiosamente, não promoveu nenhum sobressalto jurídico. Nem social. A ordem continua serena.

---

4 Ainda no RASI2020, dentre renovações e novas autorizações, surgem destacadas 8 despachos de autorização de instalação de múltiplas cameras de videovigilância para localidades. Consultáveis a partir dos Anexos do relatório, Medidas legislativas, página 15 e ss.
Nota: entretanto, no início do mês de março 2021, foi-nos dada a conhecer a autorização para instalação de mais 216 cameras de videovigilância na cidade de Lisboa, para juntar às já existentes (o Bairro Alto já dispõe de sistema, por exemplo).

5 https://expresso.pt/sociedade/2021-03-26-Portugueses-fogem-para-longe-das-restricoes-um-em-cada-dez-dormiu-a-mais-de-100-quilometros-de-casa-esta-quinta-feira-b98a7df0 (último acesso 31MAR21).

6 Vejamos, por exemplo, o detalhe dos grafos sobre a evolução do confinamento e mobilidade em: https://www.pse.pt/evolucao-confinamento-mobilidade/ (último acesso 31MAR21).

Curiosamente. Mas, não houve tratamento de dados pessoais para a revelação de tais estatísticas em mobilidade? Que finalidade jurídica prosseguiu a captura de tais dados? Que dados foram recolhidos? Foram coligidos de forma lícita? Que tratamento tiveram? Quais as garantias de anonimização e/ou minimização do tratamento?

Alguém questionou?

Alguém se indignou?

Não sendo a primeira vez que uma entidade privada analisa dados dos portugueses, em massa, sem qualquer tipo de reacção/oposição por parte destes, presumivelmente, como solução eficiente a tomar por parte do Estado, no futuro deveremos promover toda uma actividade concursal de fundos públicos para *investigação* - geral e abstrata - de *tendências, mobilidade, gostos e desejos* dos portugueses. Não que haja uma qualquer necessidade de uma finalidade concreta, lícita de sopeso. Afinal, o problema, de fundo, do sobressalto cívico e jurídico, da ordem, reside numa mera formalidade de *marketing*, o "publico não pode" vs. "privado tudo pode".

Acabemos prontamente com a folia[7].

O acesso a metadados são um problema para a acção das nossas secretas?

Do titular da acção penal, *tout court*, português?

7 Reparem na notícia: https://www.jornaldenegocios.pt/economia/impostos/amp/fisco-vai-ter-assistente-virtual-no-facebook-para-responder-as-duvidas-de-irs (último acesso 31MAR21).
Ora, a Autoridade Tributária portuguesa entende que a plataforma do Facebook é a melhor disponível *para tirar dúvidas a contribuintes nacionais.* Como todos sabemos, e somos *surpreendidos semanalmente*, o Facebook, provavelmente, já é conhecedor da informação fundamental e necessária dos seus utilizadores.
Com este *passo de modernidade* da nossa AT, na prática, ao Facebook bastar-lhe-á agrupar a informação detida à contributiva, com os rendimentos declarados, das finanças portuguesas e... *Et voila*, vitracidade completa do cidadão. (quanto será o preço de cada miríade informacional de um contribuinte concreto que a AT poderá desembolsar? Haverá já um acordo bilateral entre a entidade privada e a AT?)
É, pois, tempo de assumirmos já a cedência gratuita dos nossos dados pessoais às entidades privadas e, a partir daí, o Estado seja profícuo no controlo de todas as nossas actividades sem qualquer tipo de sobressalto jurídico ou social.

Renunciemos à recolha de torrentes de dados pessoais às entidades privadas, assumamos a bonomia do *surveillance capitalism*, encapotando o próprio "*estado de vigilância*", e vivamos felizes.

E ordeiros. Sem sobressaltos.

A justificação, para esta aceitação social passiva e dócil, por parte de uma maioria de cidadãos, refletindo, denota muito do seu analfabetismo. Analfabetismo digital. Mas também social. A ordem das coisas apenas sobrepuja o ponto de partida. A liberdade individual é gratuitamente cedida a entidades privadas. Nunca ao Estado. A compressão de direitos fundamentais apenas terá de partir deste porto privado.

Aquiesçamos, afinal, mais de duzentos anos depois, a sociedade não compreende o ditame de que "*uma sociedade que troca um pouco de liberdade por um pouco de ordem acabará por perder ambas, e não merece qualquer delas*"[8].

Nesta nova edição da Cyberlaw by CIJIC, em consonância com os docentes do Mestrado em segurança da informação e direito do ciberespaço[9], tivemos o ensejo de provocar alguns discentes a reflexões sobre a realidade pungente que convoca a sociedade. No presente e para o futuro. Entre a segurança da informação nas organizações (SiO), a consciencialização dos funcionários das organizações para a temática, o factor humano na SiO; dados pessoais em *Schrems II* e acesso a metadados por parte do MP sem um suspeito determinado ou determinável, *not/net neutrality*, os discentes procuraram reunir algumas interjeições que, como já demos conta oportunamente, ajudem a mitigar a desigual compreensão, a despertar a consciencialização individual para promoção de um combate ao analfabetismo digital.

Trazemos, também, a participação de proeminentes juristas brasileiros que acederam ao nosso convite para dissertarem sobre a lei geral de proteção de dados brasileira assim como sobre o fenómeno do *stalking* em contexto laboral inclusive em ambiente digital.

8 Thomas Jefferson (1743-1826), carta a James Madison.
9 https://fenix.tecnico.ulisboa.pt/cursos/msidc

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

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

Boas leituras.

Lisboa, FDUL, 31 de Março de 2021

Nuno Teixeira Castro

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM BREVE HISTÓRICO DE SUA CRIAÇÃO E PERCALÇOS ATÉ À VIGÊNCIA

MARCELO CRESPO *

* Advogado. É sócio no PG Advogados e um dos advogados mais respeitados no Brasil, na especialidade proteção de dados e direito digital. É Doutor e Mestre em Direito Penal pela USP. Possui especializações pela Universidade de Salamanca. É *Certified Compliance and Ethics Professional* – International (CCEP-I) pela *Society of Corporate Compliance and Ethics* (SCCE) e é Coordenador da pós-graduação em direito digital e Compliance do Damásio Educacional. É palestrante nacional e internacional e autor de diversos artigos, no Brasil e no exterior, sobre Direito Digital e Proteção de Dados.

RESUMO

Este artigo demonstra o percurso legislativo da introdução da Lei Geral de Proteção de Dados no Brasil. Para tanto, observou-se os percalços para a sua plena efetivação, desde 2010 até o presente momento, assim como os principais atos do Congresso Nacional que culminaram na promulgação da LGPD em 2018, aqui incluídas as discussões sobre o prazo de vacatio legis e a própria instituição da ANPD. Além do estudo da tramitação da lei, seguiu-se para o exame dos seus aspectos estruturantes. O artigo também aponta como a implementação da LGPD depende do porvir, em especial da efetiva atuação da ANPD e a incorporação ao cotidiano brasileiro da experiência de países avançados na proteção de dados.

Palavras-Chave: *Lei Geral de Proteção de Dados. Congresso Nacional. Vacatio Legis. ANPD. Proteção de dados pessoais.*

ABSTRACT

This article highlights the legislative path of the Lei Geral de Proteção de Dados - LGPD (Brazilian General Data Protection Law) in Brazil. Therefore, the obstacles to its full effectiveness were observed, from 2010 to the present moment, as well as the main acts of the Brazilian National Congress that resulted in the enactment of the LGPD in 2018, including debates on the deadline for the law to come into force and the ANDP implementation itself. In addition to studying about the drafting of the law, the article has analyzed its structural aspects. The article also points out how the application of the LGPD depends on what is coming, especially on the effective performance of the ANPD and the incorporation of the experience from countries with advanced data protection regulations into Brazilian daily life.

Keywords: Lei Geral de Proteção de Dados. Brazilian National Congress. Coming into Force of Legislation. ANPD. Personal data protection.

1. Um breve histórico do surgimento da LGPD

Embora o assunto tenha ganhado holofotes mais recentemente e a lei ter entrado parcialmente em vigor em setembro de 2020, a criação da LGPD é um pouco mais antiga, remetendo-nos a 2010. Naquele ano o Ministério da Justiça, na plataforma "culturadigital.br" deu início a uma consulta pública que ficou aberta por quatro meses, para que as pessoas pudessem trazer contribuições sobre o que deveria ser uma Lei Geral de Proteção de Dados Pessoais.

Com nítido embalo a partir da consulta pública, em 2012 surgiu o primeiro projeto de lei que pretendeu regulamentar a matéria, proposto pelo Deputado Milton Monti. Surgia aí o PL 4.060/12 que, todavia, só teve andamento no ano seguinte, quando o escândalo de espionagem internacional praticado pela Agência Nacional de Segurança (NSA) veio à tona por revelações de Edward Snowden. O escândalo repercutiu mundialmente, inclusive no Brasil, tendo sido alvo de críticas da então Presidente Dilma Rousseff e ajudou que o tema proteção de dados e direitos na Internet tivessem maior atenção, o que redundou na aprovação e sanção da lei 12.965/14, conhecida como "Marco Civil da Internet" (MCI). Consideramos que a aprovação do MCI foi como uma resposta à espionagem internacional, pretendendo-se demonstrar que no Brasil havia regras para a utilização da Internet.

O episódio de espionagem foi alvo até mesmo de uma Comissão Parlamentar de Inquérito no Senado, ocasião em que o PL 4.060/12 teve momentos de debate, já que, embora não pudesse evitar a espionagem, colocava o tema proteção de dados em evidência no Brasil.

Em 2015 houve uma segunda rodada de consulta pública, na mesma plataforma, do mesmo Ministério da Justiça, sendo que, ato contínuo, as contribuições foram compiladas e consolidadas, sendo o Anteprojeto enviado à Câmara dos Deputados, onde foi protocolado sob o número 5.276/16. Agora projeto de lei, o PL 5.276/16 não só era mais

amplo como também mais bem redigido que o PL 4.060/12. Por este motivo, teve apoio para tramitar mais rapidamente.

Com as Casas Legislativas em acordo sobre o tema, o PL 5.276/16 prosperou. Mas, como o Regimento Interno da Câmara dos Deputados[1] determina que os projetos mais antigos têm prioridade de tramitação, este PL foi apensado ao 4.060/12. Votados em plenário em 29 de maio de 2018, foram aprovados por unanimidade e seguiram para o Senado, lá recendo o número 53/18. No dia 03 de julho foi pautado na Comissão de Assuntos Econômicos, com a relatoria do então Senador Ricardo Ferraço, que igualmente era responsável pelo PL 330/13, que também tratava da proteção de dados pessoais.

Em audiência pública realizada na Comissão de Assuntos Econômicos, tivemos a oportunidade de contribuir como especialista, fazendo exposição oral, ocasião em que lembramos a importância do tema, além de termos defendido a ideia de que os entes públicos não fossem excluídos da lei (porque havia um início de movimento para esta exclusão) e, ainda, que a figura do encarregado de proteção de dados pudesse ser ocupada por pessoas jurídicas, uma vez que o projeto previa apenas a ocupação de cargos por pessoas físicas[2].

O texto foi votado, aprovado e enviado ao plenário em regime de urgência, de forma que, no dia 10 de julho, após fortes pressões da sociedade civil[3], o PL foi pautado e

1 O Regimento Interno é a Resolução 17 de 1989 e tem a seguinte redação no que diz respeito ao trâmite dos projetos de leis:
Art. 143. Na tramitação em conjunto ou por dependência, serão obedecidas as seguintes normas: I - ao processo da proposição que deva ter precedência serão apensos, sem incorporação, os demais; II - terá precedência: a) a proposição do Senado sobre a da Câmara; b) a mais antiga sobre as mais recentes proposições; III - em qualquer caso, as proposições serão incluídas conjuntamente na Ordem do Dia da mesma sessão.
2 Após, no final do ano de 2018, o Presidente Michel Temer, considerando nossos comentários feitos na audiência pública, editou a MP 869/18, que instituía a Autoridade Nacional de Proteção de Dados Pessoais, mudava o período de adaptação da lei, estendendo-o para agosto de 2020 e, fazendo outros ajustes, dentre eles, o de incluir pessoas jurídicas como encarregados de proteção de dados, nos termos do que comentamos na audiência pública. Participação na audiência pública disponível no link a seguir https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=13833, acesso em 14.07.2020.
3 Assinamos manifestos pela BRASSCOM, como juristas, defendendo a aprovação do PL 53/18. Documentos disponíveis em: https://docs.google.com/viewerng/viewer?url=https://brasscom.org.br/wp-content/uploads/2018/06/DOC-2018-049-Manifesto-apoio-PLC-53-18-Dados-Pessoais-v30-logos-v41.pdf&hl=pt_BR, acesso em 14.07.20.

aprovado. Na sequência, foi encaminhado para a sanção presidencial, que ocorreu em cerimônia oficial no Palácio do Planalto, em 14 de agosto de 2018[4].

Naquele dia surgia a LGPD no ordenamento jurídico brasileiro, embora ainda estivesse em período de *vacatio legis* e com alguns vetos, em especial nos artigos 55 a 59. Justamente os artigos que tratavam da Autoridade Nacional de Proteção de Dados Pessoais.

As justificativas de veto tinham como argumento o vício de iniciativa, isto é, a ANPD não poderia ser criada por iniciativa do Poder Legislativo, vez que isso feriria o princípio da separação dos Poderes. Era necessário, assim, que a ANPD fosse criada por iniciativa normativa do Poder Executivo. De todo modo, mesmo que com vetos, tínhamos o surgimento da LGPD[5].

Resumidamente, a Lei Geral de Proteção de Dados (LGPD) foi aprovada com um texto focado na proteção dos dados pessoais. Em outras palavras, protege os dados das pessoas físicas, chamados no texto legal de "titulares", visando resguardar sua privacidade. Outros tipos de dados, tais como os segredos de negócios, itens puramente financeiros, planos estratégicos, algoritmos, softwares e outros documentos ou informações que não digam respeito a uma pessoa física não são protegidos pela lei[6].

4 Estivemos presentes na cerimônia de sanção da LGPD, no Palácio do Planalto. No dia anterior à sanção, concedemos entrevista para a CBN sobre a LGPD. Disponível: https://cbn.globoradio.globo.com/media/audio/205291/se-sancionada-lei-dara-ao-cidadao-o-direito-de-ser.htm, acesso em 14.07.20.

5 Em 27 de dezembro de 2018 foi editada a Medida Provisória n° 869, publicada no Diário Oficial da União no dia seguinte, que promoveu alterações no texto sancionado e criou a ANPD. A MP foi votada no ano seguinte, tendo sido convertida em lei, recebendo o número 13.853/19.

6 Não que estes não gozem de proteção legal, no entanto são outros diplomas que serão os responsáveis por isso, tais como a lei de propriedade industrial (9.279/96), lei do software (9.609/98), lei de direitos autorais (9.610/98), entre outras.

2. Os percalços até à vigência

Costumamos dizer que o Brasil tem algumas particularidades curiosas. Para além das jabuticabas e do carnaval, gostamos de mencionar que, por aqui, até mesmo o passado é incerto. Isso porque há questões legislativas e judiciais que trazem insegurança jurídica e fazem coisas "certas e concretizadas" se transformarem em outras.

Veja-se o problema.

Apesar de aprovada desde 2018, a LGPD ainda dependia de duas coisas para que fosse efetivamente aplicada: a) o esgotamento do período do prazo de adaptação (vacatio legis); e, b) a criação da ANPD, órgão cuja principal finalidade seria a de fiscalizar a aplicação da lei.

2.1.Sobre o período de adaptação: os infindáveis debates e desdobramentos sobre a *vacatio legis*

A lei, promulgada em agosto de 2018, previa que sua entrada em vigor se daria "após decorridos 18 (dezoito) meses da sua publicação oficial", conforme art. 65 em sua versão original. No entanto, como visto, não foi posto em prática plano para operacionalizar a ANPD, o que impediu uma série de regulamentações que deveriam ser feitas pela Autoridade, tais como as hipóteses de dispensa de indicação de Encarregado de Proteção de Dados (art. 41, § 3º), a portabilidade (art. 18, V) e mesmos prazos para resposta a requisições dos titulares (art. 19, § 4º), dentre outros temas.

E, assim, como sempre há alguns posicionamentos retardantes, passou-se a discutir a inviabilidade da entrada em vigor em fevereiro de 2020 (18 meses após a publicação, conforme previa o artigo 65). Os argumentos eram de que um ano e meio não seria suficiente para colocar em operação todos os requisitos de uma lei tão abrangente quanto a LGPD. Ainda mais sem a existência concreta da ANPD.

2.2. A Medida Provisória 869/18 e sua conversão na lei

Neste processo de discussão que aconteceu no segundo semestre de 2018, foi editada a Medida Provisória (MP) 869, ainda em 2018, que realizou uma série de alterações à legislação original, sendo que em relação ao prazo de entrada em vigor, a MP dividiu os prazos em dois: os artigos referentes à ANPD entrariam em vigor em 28 de dezembro de 2018, e o restante da lei – incluindo-se então as sanções administrativas ou possibilidade de ações civis de responsabilidade, por exemplo – com vigência após 24 (vinte e quatro) meses da publicação.

Lembramos que no momento da sanção presidencial ocorreu um veto parcial (VET 24/2019), que buscava remover algumas das sanções administrativas como a suspensão parcial do funcionamento do banco de dados a que se refere a infração, suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração, e proibição parcial ou total do exercício das atividades relacionadas a tratamento de dados. Mas, como dissemos sobre o passado ser incerto, o Congresso Nacional derrubou parcialmente o veto presidencial e estes três tipos de sanções administrativas foram mantidos na LGPD, quando da conversão da MP na Lei 13.853/2019.

2.3.O projeto de lei 1.179/2020 e sua conversão na lei 14.010/20

Quando todos esperavam que os prazos previstos pela sanção da Lei 13.853/2019, alterando a Lei 13.709/2018 (LGPD), seriam “definitivos”, essas expectativas logo foram desfeitas, já que a Organização Mundial de Saúde (OMS) declarou a situação do coronavírus como uma pandemia e com ela os problemas econômicos, políticos, jurídicos e sociais se agravaram de forma generalizada. As empresas tiveram de focar em atividades essenciais para manter os negócios e a sobrevivência financeira, de forma a evitar a bancarrota e mitigar a demissão de funcionários. O sistema de trabalho presencial foi muito afetado pela pandemia, pois muitos empregados passaram a trabalhar em casa.

Diante dessa atípica situação mundial, além de a estruturação da ANPD não ter sido efetivada, vários projetos de lei foram apresentados no Congresso Nacional para tentar postergar o início da vigência da LGPD. Dentre esses, o Projeto de Lei (PL) 1179/2020, de autoria do Senador Antônio Anastasia, de Minas Gerais, proposto em 30 de março de

2020, que no meio de uma infinidade de proposições para o período excepcional da pandemia buscava, também, alterar o art. 65 da LGPD. A proposta era que a LGPD deveria entrar em vigor 36 (trinta e seis) meses após a data de sua publicação. Mas, durante o processo legislativo essa sugestão foi modificada e quando o PL foi convertido na Lei 14.010/2020, alterou apenas o prazo para as sanções administrativas, para 01 de agosto de 2021.

2.4.A Medida Provisória 959/20 e sua conversão na lei

Para tentar por fim às discussões sobre a vigência da LGPD, a MP 959/2020, editada em 29 de abril de 2020 pelo Presidente da República, corria paralelamente ao PL 1.179/2020 e veio, ao final de sua tramitação, selar o prazo para entrada em vigor dos demais artigos da lei, ou seja, aqueles que não tratam das sanções administrativas, para o dia 3 de maio de 2021.

Conforme a Constituição Federal de 1988, em caso de relevância e urgência, o Presidente da República pode adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional. No entanto, a medida provisória possui prazo de validade, devendo ser votada no Congresso e convertida em lei em até 60 dias da sua edição, prorrogáveis por mais 60 dias. Terminado esse período, ela caduca, ou seja, perde a eficácia.

Nesse sentido, para evitar que a MP caducasse, o Presidente do Senado Federal, por meio de um ato, em 26 de junho do mesmo ano prorrogou a vigência da MP 959/2020 por mais 60 dias, estabelecendo a data final de sua validade para 27 de agosto de 2020.

Nesse cenário, as incertezas quanto à MP 959/2020 eram as seguintes:

> 1) caso a MPV 959/2020 fosse aprovada pelo Congresso até 27 de agosto de 2020, a LGPD entraria em vigor em 3 de maio de 2021, com sanções a partir de 1 de agosto de 2021;

2) caso a MPV 959/2020 fosse rejeitada pelo Congresso, a LGPD entraria em vigor em sua data originalmente prevista, ou seja, 16 de agosto de 2020, com sanções a partir de 1 de agosto de 2021;

3) caso a MPV 959/2020 viesse a caducar, ou seja, caso superado o seu prazo de vigência em 27 de agosto de 2020 sem que houvesse a sua votação pelo Congresso, a LGPD entraria em vigor no dia útil seguinte, com sanções a partir de 1 de agosto de 2021;

4) caso uma das casas (Câmara dos Deputados ou Senado Federal) aprovasse uma emenda, um substitutivo à MPV 959/2020 seria votado em ambas as casas.

As indefinições perduraram até 25 de agosto de 2020, data em que a Câmara dos Deputados, levando em consideração a falta de estruturação da ANPD, aprovou um substitutivo ao texto da MP 959, definindo a data de 31 de dezembro de 2020 como o início da vigência da LGPD. Esse substitutivo, denominado de Projeto de Conversão em Lei (PLV) 34/2020, foi encaminhado ao Senado Federal e no dia seguinte, em 26 de agosto de 2020, estava submetido à votação.

Mas aí fomos surpreendidos novamente! O Presidente do Senado Federal acolheu uma questão de ordem apresentada pelo MDB para que a prorrogação da entrada em vigor da LGPD fosse considerada questão preclusa, porque já havia sido avaliada anteriormente pelo Senado, quando houve a votação do PL 1179/2020, convertido na Lei 14.010/2020 (porque a matéria de adiamento já havia sido deliberada). Assim, considerou-se o artigo 4º do PVL 34/2020 como não escrito.

Diante de toda a situação descrita anteriormente, a MPV 959/2020 manteve a sua vigência até que o texto do PLV 34/2020 fosse sancionado ou vetado pelo Presidente da República, o que deveria ocorrer em até 15 dias úteis após o seu recebimento (contado de 27 de agosto de 2020) na Casa Civil, sob pena de o PLV 34/2020 ser considerado aprovado tacitamente (sancionado, na prática).

Com a conversão, pelo Presidente da República, da MPV 959/2020 na Lei 14.058/2020, a LGPD entrou em vigor em 18 de setembro de 2020. Com isso, o artigo 65 (que trata da vigência da LGPD) constou da seguinte redação, contendo três prazos de vigência diferentes:

> 28 de dezembro de 2020 quanto aos artigos sobre a criação da ANPD (art. 55-A a 58-B), o que foi incluído pela Lei 13.853/2019;
>
> 1º de agosto de 2021 quanto à aplicação de sanções administrativas pela ANPD (arts. 52 a 54), o que foi incluído pela Lei 14.010/2020;
>
> 24 meses após a data da sua publicação, quanto aos demais artigos, o que foi incluído pela Lei 13.853/2019.

O próximo passo foi seguir com a estruturação e funcionamento da Autoridade Nacional de Proteção de dados, viabilizando suas operações, como por exemplo, regulamentar artigos da LGPD que necessitam de melhor interpretação. Dentre outras atribuições, a ANPD é responsável por receber protocolo de consultas públicas, de códigos de conduta e de códigos de melhores práticas, promover a fiscalização e o estreitamento de relacionamento com as demais autoridades.

2.5.Sobre a estruturação da ANPD

É importante destacar que a LGPD entrou em vigor sem que a ANPD estivesse funcionando de fato, já que o Decreto de sua estruturação (Decreto 10.474/2020) foi editado no dia 27 de agosto de 2020. Isso, evidentemente, torna o desafio de conformidade com a legislação mais complexo, tendo em vista que na LGPD vários pontos foram deixados sem definições específicas pelo Poder Legislativo, pendentes de futuras regulamentações pela ANPD.

A ANPD será composta por trinta e seis cargos em comissão e outras vinte funções comissionadas, todas as posições vinculadas ao Poder Executivo. Embora os cargos ainda estejam sendo preenchidos, a Autoridade já conta com uma diretoria estruturada, onde

Waldemar Gonçalves Ortunho Junior é Diretor-Presidente e Arthur Pereira Sabbat, Miriam Wimmer, Nairane Farias Rabelo Leitão e Joacil Basílio Rael compõem o conselho diretor. A nomeação feita pelo Presidente de República foi aprovada pelo Senado Federal, em 20 de outubro de 2020.

Com alguns meses de atuação, a ANPD já publicou uma Agenda Regulatória bianual (2021-2022) listando itens prioritários para atuação da Autoridade[7] , um Planejamento Estratégico para 2021-2023, em que enumera os objetivos e as ações estratégicas da Autoridade para os próximos anos, bem como foi habilitada na plataforma integrada de ouvidoria e acesso à informação "Fala.br", para facilitar a comunicação entre a Autoridade e os cidadãos.

Entre outras atribuições, caberá à ANPD fiscalizar o cumprimento da lei, elaborar as diretrizes do Plano Nacional de Proteção de Dados e aplicar as sanções administrativas nas empresas que não cumprirem a LGPD. Todavia, as penalidades administrativas somente poderão ser aplicadas a partir de agosto de 2021, conforme previsto no texto legal. Lembrando que as penalidades podem ser de advertência, publicização da infração, multas, bloqueio e eliminação dos dados pessoais tratados ilicitamente, além das suspensões dos bancos de dados e das atividades de tratamento.

Temos muita curiosidade para saber a linha de atuação que os dirigentes da ANPD irão tomar, se será um órgão que vai orientar antes de punir ou se será mais punitivo que orientativo. Aguardemos.

7 Dentre os itens prioritários, constam a regulamentação do regimento interno da ANPD; do planejamento estratégico da ANPD; da proteção de dados e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos; dos direitos dos titulares de dados pessoais; do estabelecimento de normativos para aplicação do art. 52 e seguintes da LGPD; da comunicação de incidentes e especificação do prazo de notificação; do relatório de Impacto à proteção de dados pessoais; do encarregado de proteção de dados pessoais; da transferência internacional de dados pessoais; e, das hipóteses legais de tratamento de dados pessoais (Portaria nº 11/21).

3. Um panorama sobre a LGPD

Podemos afirmar que a LGPD não tem como escopo a segurança da informação, já que sua principal preocupação é mais ampla: a privacidade dos titulares de dados pessoais. Não é, portanto, uma lei que trate de segurança da informação senão de forma tangencial.

Vejamos, rapidamente, sua estrutura:

Capítulo I – Disposições preliminares.

Capítulo II – Do tratamento de dados pessoais.

Capítulo III – Dos direitos do titular.

Capítulo IV – Do tratamento de dados pessoais pelo Poder Público.

Capítulo V – Da transferência internacional de dados.

Capítulo VI – Dos agentes de tratamento de dados pessoais.

Capítulo VII – Da segurança e das boas práticas.

Capítulo VIII – Da fiscalização.

Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Capítulo X – Disposições finais e transitórias.

A LGPD, a exemplo do RGPD, não impede o tratamento de dados de forma absoluta, tendo como objetivo que as empresas tenham uma boa governança sobre dados pessoais. Protege-se, pois, a privacidade das pessoas por meio da proteção dos dados pessoais.

Temos que a LGPD é uma lei principiológica, já que não traz minúcias sobre os processos de adequação, indicando no art. 2º seus fundamentos (o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais).

No art. 6º encontramos os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Já no art. 7º a LGPD trouxe as hipóteses legais de tratamento dos dados pessoais, que são o consentimento do titular, a execução de obrigação legal ou regulatória pelo controlador, a execução de política públicas pela Administração Pública, a realização de estudos por órgão de pesquisa, a execução de contrato ou procedimentos preliminares, o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, a proteção da vida ou incolumidade física de alguém, para a tutela da saúde, para atender interesses legítimos do controlador ou de terceiro e, por fim, para a proteção do crédito. No art. 11 temos as bases legais para o tratamento dos dados sensíveis, que são também o consentimento, o cumprimento de obrigação legal ou regulatória, a pesquisa realizada por órgãos de pesquisa, a proteção da vida ou incolumidade física do titular ou terceiro, a tutela da saúde, o exercício regular de direitos inclusive em contratos ou processos administrativos, judiciais ou arbitrais, bem como o tratamento compartilhado de dados pela Administração Pública para a execução de políticas públicas e, por fim, a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Sobre os direitos dos titulares, deve-se olhar especialmente para o art. 18. Basicamente são o direito de confirmação da existência, acesso aos dados, correção, anonimização, portabilidade, eliminação, informação das entidades com as quais há tratamento compartilhado, além da informação sobre a possibilidade de não fornecer o

consentimento e as consequências disso, além da evidente possibilidade de revogação do consentimento.

Sobre segurança, o art. 46 a LGPD determina que os "agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Ou seja, impõe a adoção de medidas técnicas para a proteção de dados pessoais, sem, no entanto, dizer quais são as ferramentas adequadas para isso.

Por fim, no art. 50 traz disposições sobre o que deveria ser um programa de *privacy compliance*. A redação não e das melhores porque dá a entender que o programa é uma possibilidade, não uma obrigatoriedade. Apesar disso, determina que, havendo o programa, devem ser respeitados seus elementos mínimos que são os seguintes: a demonstração do comprometimento do controlador em adotar processos e políticas que assegurem o cumprimento das normas e boas práticas de proteção de dados pessoais, a aplicação do programa a todo o conjunto de dados pessoais que estejam sob seu controle, a adaptação à estrutura, escala e ao volume das operações e sensibilidade dos dados, o estabelecimento de políticas e salvaguardas baseados em avaliação sistemática de risco, a busca pelo estabelecimento de relação de confiança com o titular dos dados, a integração com a estrutura geral de governança com mecanismos de supervisão internos e externos, a existência de plano de resposta a incidente e remediação e, ainda, que seja atualizado constantemente.

4. Considerações Finais

A LGPD é a Lei Geral de Proteção de Dados Pessoais do Brasil que, como muito do que vivemos por aqui, surgiu após momentos controvertidos, haja vista todo o percalço legislativo que tratou da sua vacatio legis. Trata-se de importante legislação com clara inspiração no Regulamento Geral de Proteção de Dados Pessoais, embora seja menos extensa, contenha menos normas e seja menos detalhista em procedimentos. Sendo assim, sua aplicação tenderia a ser menos complexa que o RGPD.

Temos, no entanto, uma boa desvantagem sobre como deve ser a aplicação da lei, tendo-se em visto que o tema "proteção de dados" é muito mais recente no Brasil que na União Europeia, assim, teve menos tempo de maturação.

Estamos também, ainda na dependência da efetiva operação da ANPD, já que seus diretores foram empossados no final do ano de 2020 e a Autoridade ainda está iniciando os trabalhos. Há um sentimento, por hora, de muita expectativa e esperança de que a ANPD possa trazer importantes regulamentações sobre a proteção de dados e que possa agir como um órgão de *enforcement*. Isso para que não enfrentemos o velho problema brasileiro das "leis que não pegam" (que não são aplicadas).

Estamos no caminho certo para melhorar o contexto da privacidade e da proteção de dados pessoais. Mas ainda há muito trabalho pela frente. Esperamos que seja possível absorver boas e más experiências de países que, antes do Brasil, puderam efetivar a proteção de dados pessoais.

5. Referências Bibliográficas

BENNETT, Colin J.; RAAB, Charles D. The Governance of Privacy: Policy Instruments in Global Perspective. Reino Unido: Routledge, 2017.

BOVENS, M. Analysing and assessing accountability: A conceptual framework 1. European law journal. 2007 Jul;13(4):447-68.

BRASIL. Senado Federal. Senado confirma primeira diretoria da Autoridade Nacional de Proteção de Dados. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados, acesso em 23.03.2021.

CRESPO, Liana Irani Affonso Cunha. Interação com terceiros e due diligence. In: Governança, Compliance e Cidadania. 2ª Edição. Revista dos Tribunais: São Paulo, 2019.

_____, et al. A importância do Tone At The Top e os seus Desafios na Prática. In: Guia Prática de Compliance. Org. Isabel Franco. Forense. Rio de Janeiro, 2020.

CRESPO, Marcelo Xavier de Freitas (Coord). Compliance no Direito Digital. São Paulo: Thomson Reuters, 2020

_____. Compliance Digital. In: Governança, Compliance e Cidadania. 2ª Edição. Revista dos Tribunais: São Paulo, 2019.

_____. Compliance Digital. In: Governança, Compliance e Cidadania (Irene Patrícia Nohara e Flávio Leão Bastos Pereira, coordenadores). Editora Thomson Reuters: São Paulo, 2018.

_____; BELOTO, Guilherme. Brazil's general data protection law: What has it done? Disponível em https://compliancecosmos.org/brazils-general-data-protection-law-what-has-it-done?authkey=c5f558d77cdb50c4627dd8c91d3e572eb21b7c5a20a28ccce8725126ddb15415,

_____; BELOTO, Guilherme. Privacy compliance challenges in 2020 and beyond. Disponível em: https://compliancecosmos.org/privacy-compliance-challenges-2020-and-beyond, acesso em 25.03.21.

_____. Privacy Compliance: A View from Brazilian General Data Protection Law (LGPD). In: MAKOWICZ, Bartosz (coordenador). Yearbook of Global Ethics, Compliance and Integrity. Recht Wirtschaft Steuern, 2020.

CROMPTON, Malcolm. TROVATO, Michael. The New Governance of Data and Privacy: Moving beyond compliance to performance. Austrália: Australian Institute of Company Directors, 2018.

DENSMORE, Russel. Privacy Program Management. Tools for Managing Privacy Within Your Organization. Estados Unidos: IAPP, 2019.

FOX, Thomas. The Compliance Handbook, 2018.

HILL, David G. Data Protection: Governance, Risk Management, and Compliance. Estados Unidos: CRC Press, 2019.

KYRIAZOGLOU, J. Data Protection and Privacy Management System. Data Protection and Privacy Guide. Reino Unido: Bookboon, 2016. b.

LIMA, Ana Paula Moraes Canto de; CRESPO, Marcelo PINHEIRO, Patricia Peck. LGPD APLICADA. São Paulo: Atlas, 2021.

MULGAN, R. 'Accountability': An ever-expanding concept? Public administration. 2000;78(3):555-73. Disponível em https://crawford.anu.edu.au/pdf/staff/richard_mulgan/MulganR_02.pdf, acesso em 14.07.20.

SALDANHA, Nuno. RGPD – Guia Para Uma Auditoria de Conformidade, Dados, Privacidade, Implementação, Controlo e Compliance. Portugal: FCA, 2019.

Se sancionada, lei dará ao cidadão o direito de ser informado sobre o uso de seus dados. CBN Noite Total – Entrevista com Marcelo Crespo. Disponível em https://cbn.globoradio.globo.com/default.htm?url=%2Fmedia%2Faudio%2F205291%2Fse-sancionada-lei-dara-ao-cidadao-o-direito-de-ser.htm, acesso em 14.07.20.

CYBERLAW
by CIJIC

ANÁLISE E MEDIDAS DE COMBATE AO *"STALKING"* NAS RELAÇÕES DE TRABALHO INCLUSIVE EM AMBIENTE DIGITAL

VALÉRIA REANI RODRIGUES GARCIA *

e

TATIANA VEIGA OZAKI BOCABELLA*

* Advogada, com curso de extensão em "*Strategic Thinking*" pela University a Albany (State University of New York). Especialista em Direito e Privacidade de Dados Pessoais pela UNL – Universidade Nova Lisboa – Portugal. Especialista em Direito Digital e Compliance pela Faculdade Damásio Educacional. Especialista em Gestão Empresarial pela PUCC – Pontifícia Universidade Católica de Campinas e em Direito do Trabalho e Direito Processual do Trabalho pela Escola Superior de Advocacia – ESA/SP. Coordenadora Pedagógica, Científica e Docente dos cursos de Direito Digital e Inovação da ESA – Escola Superior de Advocacia de Santos, Santo André e Campinas. Presidente da Comissão Especial de Privacidade e Proteção de dados Pessoais, 2020 até então e Vice Presidente da Comissão de Direito Digital ambos os cargos de indicação na OAB Campinas e Membro Convidada do Instituto Nacional de Proteção de Dados -INPD

* Advogada. Especialista em Direito Digital e Compliance pela Faculdade Damásio Educacional. Extensão em Proteção de Dados pela Faculdade de Direito da UNL - Universidade Nova de Lisboa - Portugal, extensão em Direitos Sociais pela Faculdade Católica de Lisboa - Portugal, extensão em Compliance pela FVG - Fundação Getúlio Vargas, extensão em Direito Digital e Proteção de Dados pela PUC/SP – Pontifícia Universidade Católica de São Paulo.

RESUMO

Este artigo se propõe a analisar a ocorrência do *stalking* nas relações de trabalho, conceituando o instituto, discorrendo sobre as formas como o *stalking* pode ser praticado e, mais especificamente, como ele é cometido na esfera laboral, exemplificando condutas que podem caracterizá-lo, quais os requisitos para que seja individualizado, as consequências de sua ocorrência para a vítima, formas jurídicas de reparação e apresentar medidas e estratégias que podem ser adotadas como forma de coibir a prática do *stalking* e *cyberstalking.*

Palavras-Chave: *stalking*, assédio persistente, perseguição, relações de trabalho, consequências.

ABSTRACT

This article aims to analyze the occurrence of stalking in labor relations, conceptualizing the institute, discussing the ways in which stalking can be practiced and, more specifically, how it is committed in the labor sphere, exemplifying conducts that can characterize it, what the requirements for it to be individualized, the consequences of its occurrence for the victim, legal forms of reparation and present measures and strategies that can be adopted as a way to characterize the practice of stalking and cyberstalking.

Keywords: stalking, persistent harassment, persecution, work relationships, consequences.

Introdução

O presente artigo visa analisar de que forma o *stalking* pode ocorrer nas relações de trabalho, demonstrando que não é uma conduta exclusiva do mundo das celebridades, e que é mais comum do que se possa imaginar.

O *stalking* se caracteriza por um conjunto de condutas reiteradas, praticadas de forma perturbadora contra a vítima (na grande maioria das vezes, mulheres), como meio de perseguição obsessiva, razão pela qual também pode ser conhecido como assédio por intrusão ou assédio persistente.

O assunto não é novo. Muito provavelmente, desde que o mundo existe e as pessoas convivem em sociedade, o *stalking* é praticado.

Trata-se de uma conduta que era muito conhecida e evidenciada no mundo artístico, com as celebridades, embora não com essa nomenclatura. São inúmeros os casos de *stalking* ocorridos nesse meio, e que se tornaram mundialmente conhecidos. Um caso famoso de *stalking* é a tentativa de assassinato do presidente americano Ronald Reagan, cometida por John Hinckley Jr, em 1981. Após assistir o filme *Taxi Driver*, ele ficou tão obcecado pela atriz Jodie Foster, que começou a persegui-la com telefonemas, cartas e bilhetes. Ao tentar assassinar o presidente, o objetivo era impressionar a atriz. O *stalker* foi absolvido por motivo de insanidade mental e permanece confinado em hospital psiquiátrico desde então (VITELLI, 2012).

Em decorrência de inúmeros casos de *stalking* que estavam ocorrendo, o estado da Califórnia criminalizou a conduta em 1990 e diversos outros países compilaram leis penais contra o *stalking*.

A conduta de *stalking* passou a ser mais conhecida com essa nomenclatura na década de 90 e, juridicamente falando, passou a ser adotada posteriormente, nos anos 2000.

No Brasil, o pioneiro a tratar sobre o tema foi o saudoso Prof. Damásio de Jesus, que, resumidamente, definia o *stalking* como uma forma de violência na qual o sujeito ativo invade a esfera de privacidade da vítima, repetindo incessantemente a mesma ação por maneiras e atos variados, empregando táticas e meios diversos e vai ganhando, com isso, poder psicológico sobre o sujeito passivo, como se fosse o controlador geral dos seus movimentos.

A conduta caracterizadora pode ser motivada por diversos fatores, tais como: ódio, inveja, vingança, amor platônico, dentre outras, e vai desde práticas aparentemente menos graves e inofensivas, ou mesmo de cunho afetivo, tais como mensagens amorosas e abordagens com propostas de relacionamento, até agressões físicas, ofensas morais, ameaças, violações sexuais e até mesmo a morte.

Importante destacar que hoje vivemos num mundo repleto de tecnologias e modernidades, que proporcionam facilidades que permitem a conexão constante e incessante com todos os meios, inclusive com o trabalho, e tal situação viabiliza ainda mais a ocorrência de atitudes caracterizadoras do *stalking*, inclusive e principalmente nos meios digitais (*cyberstalking)*.

Para a vítima de *stalking*, inúmeras são as consequências desse assédio, como abalos emocionais e psicológicos, insônia, desmotivação e outros problemas que, persistentes, podem inclusive levar a vítima ao suicídio.

Daí a importância e a necessidade de uma vítima de *stalking* adotar determinadas providências que possam minimizar os efeitos dessa conduta devastadora e penalizar o agressor da maneira adequada, seja civilmente, seja criminalmente.

1. Conceito de *Stalking*

O termo *stalking* (sem tradução para a língua portuguesa) deriva da palavra de origem inglesa *stalk*, que significa “espreitar a caça". Trazido para as relações humanas e pessoais, podemos entender que o termo tem o significado de perseguir.

De acordo com o tradicional dicionário jurídico americano *Black’s Law Dictionary*[1], o *stalking* pode ser caracterizado como (1) o ato ou instância de seguir alguém furtivamente; (2) o delito de seguir ou demonstrar-se perto de alguém, com o propósito de importunar ou assediar essa pessoa, ou de cometer outro crime associado, como lesão psicológica ou corporal.

O Instituto Nacional de Justiça dos Estados Unidos[2] configura o *stalking* como sendo um comportamento repetido dirigido a uma pessoa, com objetivo de efetuar contato não desejado através da comunicação ou de ameaças que causam alarme e medo no alvo.

Nas palavras do doutrinador Jorge Trindade, “trata-se de uma constelação de condutas que podem ser muito diversificadas, mas envolvem sempre uma intrusão persistente e repetida através da qual uma pessoa procura se impor à outra, mediante contatos indesejados, às vezes ameaçadores, gerando insegurança, constrangimentos e medo na vítima”.

Na doutrina portuguesa, o *stalking* passou a ser definido como assédio persistente, um padrão de comportamentos que se traduz em formas diversas de comunicação, contato, vigilância e monitorização de uma pessoa-alvo que, pela sua persistência e contexto de ocorrência, constitui-se como uma verdadeira campanha de assédio que, muitas vezes, afeta significativamente o bem-estar da vítima. (MATOS e GRANGEIA, 2011).

Assim, pode-se dizer que o *stalking* nada mais é do que a perseguição obsessiva, insistente e doentia praticada por uma pessoa (conhecida como

1 *In* AMIKY, Luciana Gerbovic.
2 *In* MARCHESI, Sephora.

stalker) contra determinada vítima, por meio de reiterada conduta perturbadora, o que faz com que seja chamado, também, de assédio por intrusão.

Assim, por meio do *stalking*, o *stalker* (perseguidor) impõe terror psicológico à vítima e, como consequência, torna-se controlador geral de seus movimentos.

2. Meios pelos quais pode ser praticado, Tipos de conduta que caracterizam o *Stalking* e requisitos de caracterização.

O *stalking* pode ser praticado por qualquer meio, inclusive o virtual, quando então ele passa a ser conhecido como *cyberstalking*.

E as condutas e/ou comportamentos que caracterizam o *stalking* são diversas, sendo muito difícil delimitá-las, pois pode tratar-se de conduta menos grave ou mesmo de cunho afetivo, que aparentemente são inofensivas, como, por exemplo, telefonemas, envio de mensagens, envio de presentes não solicitados, dentre outras. Mas também pode referir-se a condutas mais danosas e intimidatórias, como perseguição, ofensas morais, ameaças, agressões físicas e mesmo a morte.

Entretanto, não basta simplesmente a prática das condutas acima mencionadas. Ou seja, se elas forem praticadas de forma isolada ou pontual, não se caracteriza o *stalking*.

Para que tais ações sejam caracterizadas como *stalking*, é necessário que as condutas praticadas, de qualquer forma, sejam incomodativas, desagradáveis, inconvenientes, insistentes e reiteradas, colocando a vítima em situação de constrangimento, de intimidação, de violabilidade de sua intimidade.

3. Sujeitos do *Stalking*

Podemos concluir que os sujeitos do *stalking* são quaisquer pessoas, tanto homens como mulheres, mas estatisticamente (SPITZBERG, 2002) as mulheres (75%) são a maioria no polo passivo, como vítimas, e os homens (79%) no polo ativo, como *stalkers* (perseguidores).

Boen e Lopes descrevem em seu artigo algumas estatísticas mais precisas, informando que, de acordo com Patricia Tjaden e Nancy Thoennes (1998), 59% das mulheres foram vítimas de *stalking* por parte de um parceiro íntimo e 81% dessas mulheres também foram fisicamente agredidas. Já Brian Spitzberg e William Cupach (2007), informam que aproximadamente 80% dos *stalker* são conhecidos da pessoa que eles perseguem. Ainda, Rosemary Purcell, Michele Pathé e Paul E. Mullen (2000 *apud* WELLER et al., 2012) apresentam que, aproximadamente, 50% dos casos de *stalking* envolvendo ofensores desconhecidos com frequência possuem a duração de apenas alguns dias e, comumente, não são mantidos por mais de duas semanas.

4. *Stalking* – Relação laboral e o ordenamento jurídico trabalhista brasileiro

Superadas essas considerações preliminares, para contextualizar o assunto, passa-se a tratar do *stalking* nas relações de trabalho.

Nesse sentido, justamente por falta de nomenclatura adequada do termo *stalking*, que não tem tradução para o português, aplicável aos casos jurídicos, os magistrados e doutrinadores do Direito do Trabalho tem entendido que o *stalking* nas relações laborais são uma espécie de assédio moral.

Assim, o *stalking* no âmbito do trabalho pode ser entendido como processo de exposição repetitiva e prolongada do trabalhador a condições humilhantes e degradantes e a um tratamento hostil no ambiente de trabalho, debilitando sua saúde física e mental (FERREIRA, 2010.)

A doutrinadora Sônia Mascaro Nascimento o define como sendo uma conduta abusiva, de natureza psicológica, que atenta contra a dignidade psíquica, de forma repetitiva e prolongada, e que expõe o trabalhador a situações humilhantes e constrangedoras, capazes de causar ofensa à personalidade, à dignidade ou à integridade psíquica, e que tem por efeito excluir o empregado de sua função ou deteriorar o ambiente de trabalho (NASCIMENTO, 2011).

Então, o *stalking* pode ser entendido como toda e qualquer conduta abusiva, tais como: gestos, palavras, escritos, comportamentos, atitudes, etc., e que, intencional e frequentemente, fira a personalidade, a dignidade e a integridade física ou psíquica de uma pessoa, ameaçando seu emprego ou degradando o clima no ambiente de trabalho.

Ainda citando Sônia Mascaro Nascimento, poderíamos exemplificar o *stalking* no ambiente de trabalho como: "(I) desaprovação velada e sutil a qualquer comportamento da vítima; (II) críticas repetidas e continuadas em relação à sua capacidade profissional; (III) comunicações incorretas ou incompletas quanto à forma de realização do serviço, metas ou reuniões, de forma que a vítima sempre faça o serviço de forma incompleta, incorreta ou intempestiva, e ainda se atrase para reuniões importantes; (IV) apropriação de ideias da vítima para serem apresentadas como de autoria do assediador; (V) isolamento da vítima de almoços, confraternizações ou atividades junto aos demais colegas; (VI) descrédito da vítima no ambiente de trabalho mediante rumores ou boatos sobre a sua vida pessoal ou profissional; (VII) exposição da vítima ao ridículo perante colegas ou clientes, de forma repetida e continuada; (VIII) alegação pelo agressor, quando e se confrontado, de que a vítima está paranoica, com mania de perseguição ou não tem maturidade emocional suficiente para desempenhar as suas funções; e (IX) identificação da vítima como "criadora de caso" ou indisciplinada".

Diante disso, importante destacar que o *stalking* não é um ato isolado, mas pressupõe um processo repetitivo e consecutivo, tendo como requisitos:

- repetição sistemática – a conduta é repetitiva, insistente, se prolonga no tempo;

- intencionalidade – tem o intuito claro de desestabilizar a vítima emocionalmente, causar-lhe um transtorno psicológico, imputar-lhe terror;
- direccionalidade – é praticado contra pessoa determinada, a vítima é escolhida "a dedo", e a partir de então todas as condutas são direcionadas exclusivamente a ela;
- temporalidade – no âmbito do direito do trabalho, pressupõe a ocorrência dentro da jornada laboral, por dias, meses, prolongando-se no tempo;
- degradação do ambiente de trabalho, com intuito de causar tanto constrangimento à vítima que a faça deixar o local, muitas vezes, de modo definitivo.

Destaque-se, também, que no ambiente laboral o *stalking* possui algumas vertentes:

- Vertical descendente – aquele praticado de cima para baixo, do superior hierárquico contra o subordinado, do empregador para com o empregado. É a forma mais comum de *stalking* no ambiente laboral. O *stalker*, por ocupar uma posição hierárquica superior, aproveita-se da condição de subordinação e de inferioridade da vítima (empregado), para não dizer de sua debilidade, para praticar atos ofensivos e humilhantes;
- Horizontal –aquele praticado por colega de mesmo nível hierárquico, ou seja, os sujeitos ativo e passivo (*stalker* e vítima) encontram-se em igualdade hierárquica no ambiente de trabalho. Um exemplo clássico desse tipo de *stalking* é quando as pessoas estão participando de um processo seletivo interno, disputando um cargo melhor, visando uma promoção profissional;
- Vertical ascendente – aquele praticado de baixo para cima, ou seja, do empregado contra o superior hierárquico. É causado por uma pessoa de nível hierárquico menor (subordinada) contra seu superior. É mais difícil de ser observado, na prática, mas um exemplo desse tipo de assédio é quando um funcionário é promovido, sem qualquer consulta dos demais colegas, e não é aceito como superior imediato, o que passa a

causar atritos entre as pessoas, pela falta de aceitação da nova posição ocupada pelo antigo colega de trabalho;

- Misto – quando é realizado por uma pluralidade de agentes, de diversos níveis hierárquicos, ou seja, a vítima sofre o assédio tanto de um colega de trabalho de mesmo nível hierárquico, quanto de um superior a quem está subordinada. Um exemplo bem característico é quando o chefe ou superior desqualifica a vítima perante os colegas e dá oportunidade para que os demais façam a mesma coisa, sem qualquer penalidade.

Adiante, passa-se a tratar das consequências do *stalking.*

5. Consequências do *Stalking*

É indiscutível que a vítima de *stalking* tenha consequências dessa perseguição refletidas na sua vida laboral, podendo estender-se, também, para a vida social e pessoal.

O *stalking* gera inúmeras consequências para o trabalhador, seja no âmbito do trabalho, seja na vida pessoal, incluindo, mas não se limitando, à queda de produtividade da vítima, o retrocesso econômico, tendências ao alcoolismo, perturbações mentais, insônia, queda da libido, lesões à saúde, involução social, danos psicológicos, isolamento, descontrole emocional, depressão e, em casos mais agudos até mesmo o suicídio, entre outros.

MOROSO, citando Mago Graciano de Rocha Pacheco[3], destaca que o sujeito passivo pode vir a sofrer de uma desestabilização grave e de alterações emocionais e de personalidade que afetam a sua saúde, influenciando a sua própria família e as relações sociais, sendo que esses efeitos nocivos podem vir a repercutir-se na organização que permite este fenômeno, e que, em geral, repercutirão sobre a sociedade.

3 PACHECO, MAGO GRACIANO de ROCHA “O Assédio Moral no Trabalho: "O Elo Mais Fraco", Coimbra, Almedina, 2007

Daí a importância de se combater essa conduta, através das medidas adequadas.

6. Providências que podem ser adotadas pelas vítimas de *Stalking* laboral e formas de reparação

Não obstante a imperiosa proteção à dignidade prevista em diversas legislações, o Brasil não possui leis específicas e determinadas que versem sobre o *stalking*, sua erradicação e efetiva proteção às vítimas.

Porém, a nossa Constituição Federal, estabeleceu como fundamentos da República Federativa do Brasil uma série de preceitos que necessariamente devem ser observados, dentre os quais, destacam-se a "dignidade da pessoa humana" e "os valores sociais do trabalho e da livre iniciativa".

Além disso, a Constituição Federal também estabeleceu, em seu artigo 170, que "a ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social".

Nesse sentido, a vítima de *stalking* no ambiente do trabalho, pode adotar algumas atitudes para reparar a violência sofrida e repreender o agressor. Uma das alternativas é o pedido de rescisão indireta, na qual a vítima fundamenta a justa causa do empregador, com amparo nas alíneas "a", "b" e "c" do art. 483, da CLT – Consolidação das Leis do Trabalho4, quando lhe forem exigidos serviços superiores às suas forças, defesos por lei, contrários aos bons costumes, ou alheios ao contrato; quando for tratado pelo empregador ou por seus superiores hierárquicos com rigor excessivo; quando correr perigo manifesto de mal considerável.

4 Decreto-Lei nº 5.452, de 1º de maio de 1943

Há, também, a possibilidade de pedir a demissão por justa causa do agressor, com fulcro no art. 482, alínea "b", da CLT, por incontinência de conduta ou mal procedimento.

Na Justiça do Trabalho também é possível pedir a reparação por danos materiais (despesas havidas com tratamentos, medicamentos, etc., bem como lucros cessantes decorrentes de valores que deixar de receber, porque muitas vezes as sequelas causadas no trabalhador são tão grandes, que a vítima não consegue se manter no mercado de trabalho e acaba deixando de receber salário, por exemplo), além de danos morais, por violação aos direitos da personalidade, autoestima, boa-fama, imagem, honra e dignidade.

A indenização por danos morais encontra-se fixada no art. 223-G da CLT, sendo que o valor varia de três vezes a cinquenta vezes o último salário contratual do ofendido, dependendo na natureza do dano (leve a gravíssima).

Conforme pontua Sônia Mascaro Nascimento:

> *"de acordo com os arts. 932, III, 933, 934 e 935 do Código Civil vigente, os quais devem ser combinados com os arts. 1.521, III, 1.522 e 1.523 do mesmo diploma legal, o empregador responde pelos danos que causar a terceiros em decorrência de obrigação contraída pela emprega, firmando relações jurídicas nacionais ou internacionais, por atos praticados por seus empregados ou prepostos, nacionais ou estrangeiros, com fundamento nas culpas in vigilando e in eligendo."* (NASCIMENTO, 2011, p. 165)

Assim, ainda que o *stalking* seja praticado por um outro funcionário da empresa, fato é que o empregador responde pelos atos de seus prepostos, conforme entendimento dos arts. 932 a 935 do Código Civil[5], entendimento este sumulado pelo Colendo STF (Supremo Tribunal Federal), na Súmula 341, *in verbis:*

> Súmula 341. É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto.

O *stalking* ainda é passível de reparação na esfera cível, em conformidade ao que prevê o art. 927 do Código Civil, senão vejamos:

5 Lei nº 10.406, de 10 de janeiro de 2002.

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187)6, causar dano a outrem, fica obrigado a repará-lo.
>
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

E, em decorrência dessa reparação, pode-se pedir a indenização por danos morais e materiais, sendo que esta última se mede pela extensão do dano (art. 944, do Código Civil).

Conforme entendimento de Nelson Nery Jr. e Rosa Maria de Andrade Nery (2013), comentando o art. 944 do Código Civil:

> *"Obrigação de indenizar. A regra é a de que quem estiver obrigado a reparar um dano deve recompor a situação pessoal e patrimonial do lesado ao estado anterior, para torná-la como era se o evento maléfico não tivesse se verificado, evento esse que impõe ao responsável pelo dano (com ou sem culpa pela sua ocorrência – dependendo da hipótese legal de que se trata) a obrigação de repará-lo. Quando o CC 944 cuida de fixar o valor da indenização pela extensão do dano, revela comando de que a obrigação deve ser cumprida pontualmente, ou seja, "ponto por ponto". Quando se diz que uma obrigação deve ser cumprida "pontualmente", diz-se que o obrigado deve satisfazer. "cabalmente, todos os deveres dela resultantes*".

Os danos morais, por sua vez, têm previsão, também, no art. 5º, incisos V e X, da Constituição Federal, que assim estabelecem:

> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O *stalking* também é passível de reparação na esfera criminal, seja como condutas menos gravosas, enquadradas como contravenção penal (ex: perturbação da tranquilidade – art. 65, LCP – Lei de Contravenções Penais), seja como crimes mais graves, como: crimes contra a honra (injúria, calúnia, difamação – arts. 138, 139 e 140 do Código Penal), crimes contra a liberdade

6 Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

individual (constrangimento ilegal e ameaça – arts. 146 e 147 do Código Penal), crimes contra a dignidade sexual (art. 216-A do Código Penal), dentre outros.

Vale destacar que o *stalking* ainda não é legalmente tipificado como crime no Brasil, mas o país ao menos já se adiantou na criação das chamadas "Medidas Protetivas de Urgência", que podem ser aplicadas em casos de *stalking* envolvendo violência doméstica e familiar contra a mulher, nos estritos termos dos artigos 5º, I a III; 7º, I a V; 11; 12, III e 22 I a V; 23, I a IV e 24, I a IV, todos da Lei 11.340/06 – Lei Maria da Penha.

CABETTE destaca em seu artigo que a prisão preventiva como instrumento para efetivar o cumprimento de medidas protetivas de urgência (art. 313, IV, Código de Processo Penal) deve ser vista não somente como um caso de aplicação de prisão provisória, mas também como fundamento desta, a fim de garantir o cumprimento efetivo das medidas protetivas de urgência e somente então reclamando do artigo 312, CPP os requisitos da prova do crime e dos indícios suficientes de autoria, destacando que a conduta do s*talking* também se amoldaria ao fundamento da preventiva previsto no artigo 312, CPP, da "garantia da ordem pública", certamente abalada com a atuação reiterada do infrator.

Além disso, já existem Projetos de Lei para que o *stalking* seja criminalizado no Brasil, como o PL 1.414/19, que prevê a alteração do art. 65 da Lei de Contravenções Penais, para quem "molestar alguém, por motivo reprovável, de maneira insidiosa ou obsessiva, direta ou indiretamente, continuada ou episodicamente, com o uso de quaisquer meios, de modo a prejudicar-lhe a liberdade e a autodeterminação", passível de prisão simples de 2 a 3 anos.

Há também o PL 1.369/19, que prevê a inserção do art. 149-B no Código Penal, para tipificar o crime de perseguição.

Referido Projeto de Lei foi aprovado pelo Senado Federal na data de 09 de março deste ano, com uma sub-emenda substitutiva global, tendo sido sancionado pelo Presidente Jair Bolsonaro, em 31 de março, **LEI Nº 14.132, DE**

31 DE MARÇO DE 2021[7] acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais) e prevê a inclusão do art. 147-A ao Código Penal, revogando o art. 65 da Lei de Contravenções Penais.

A redação aprovada pelo Senado tem a seguinte tipificação:

> Perseguição obsessiva
> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

O senador Rodrigo Cunha destacou a importância da nova tipificação, citando que a Organização Mundial da Saúde (OMS), em 2017, apontava o Brasil como o país com a quinta maior taxa de feminicídios por 100 mil mulheres em todo o mundo, sendo que 76% dos feminicídios do país são cometidos por pessoas próximas à vítima.

Ainda, foram estabelecidos os casos de agravamento da pena, que podem levá-la a ser aumentada em até 50%: se o crime for cometido contra criança, adolescente ou idoso; contra mulher por razões da condição de sexo feminino; mediante concurso de duas ou mais pessoas; ou com o emprego de arma. senão vejamos:

> § 1º A pena é aumentada de metade se o crime é cometido:
> I - contra criança, adolescente ou idoso;
> II - contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
> III - mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

Se houver outro tipo de violência, a pena de perseguição será somada à correspondente ao ato violento:

> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.

---

7 **LEI Nº 14.132, DE 31 DE MARÇO DE 2021,** Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14132.htm . Último acesso Março2021

Com isso, espera-se que as pessoas propensas a praticar o *stalking* reavaliem suas atitudes, de modo a não causarem mais prejuízos às suas vítimas.

7. Casos de *Stalking* no âmbito trabalhista

Dentro do âmbito trabalhista, vale destacar uma notícia publicada em 15 de abril de 2020, em que uma empresa foi condenada a indenizar uma trabalhadora, que foi vítima de *stalking* praticado por outro colega de trabalho[8].

Analisando a decisão, a desembargadora Silene Coelho, do Tribunal Regional da 18ª Região, entendeu que ficou comprovado que outro trabalhador perseguia a atendente, configurando um caso típico de *stalking* e condenou a empresa ao pagamento de R$ 10.000,00 (dez mil reais) por danos morais.

Destaca-se a ementa da decisão:

> ASSÉDIO MORAL. STALKING. No assédio moral, na modalidade stalking, o assediador (stalker), dentre outras condutas, invade a privacidade da vítima de forma reiterada, causa danos à integridade psicológica e emocional do sujeito passivo, lesa a sua reputação, altera do seu modo de vida e causa restrição à sua liberdade de locomoção. No caso em tela, demonstrado que o stalker, vigiava os passos, controlava os horários e tirava fotos da reclamante quando acompanhada de outros homens, para dizer que estava traindo seu marido, faz jus à indenização por danos morais em razão do assédio moral sofrido, sendo o empregador responsável de forma objetiva, consoante art. 932, III do CC/02.

E, ainda, o trecho abaixo transcrito:

> Apresenta-se, o caso em tela, como uma variável do assédio moral, na medida em que restou demonstrado que o Sr. Gabriel perseguia a reclamante em caso típico de stalking. Emerge do depoimento da primeira testemunha conduzida pela reclamante:
>
> "(...) *que o relacionamento do Gabriel e da reclamante era tenso; que o Gabriel tirava fotos da reclamante em diversas situações e fazia anotações no que a depoente não via que anotações computador; eram essas, ele deixava claro que tinha intenção de prejudicar a reclamante, sobretudo tirando fotos dela com homens para dizer que ela traía o marido; que a reclamante comunicou o fato para a supervisora e esta comunicou ao IDTECH; que todos no local, inclusive os médicos, sabiam*

8 Disponível em https://www.direitonews.com.br/2020/04/empresa-indenizar-empregada-stalking-colega-trabalho.html

> *da situação, que era muito constrangedora; que a supervisora mandou um e-mail para o IDTECH e a depoente não sabe dizer se foi tomada*".
>
> No tocante à responsabilização do primeiro reclamado ante os atos do empregado Gabriel, o art. 932, III do CC estipula a responsabilidade objetiva, sendo despicienda a análise de conduta patronal.
>
> Ainda que assim não fosse, a prova oral demonstrou o conhecimento do primeiro reclamado, haja vista que foi enviada a notícia dos acontecimentos ao IDTECH, pelo que se manteve internet, incidindo sua responsabilidade na modalidade culposa, porquanto tem o dever de manter o meio ambiente de trabalho também psicologicamente sadio.
>
> Quanto ao valor da indenização, a despeito da legislação trabalhista ter sido taxada no quesito da fixação, trouxe na norma do art. 223-G da CLT em seus incisos verdadeiros nortes ao operador do direito.
>
> No caso em tela, o Gabriel, além de violar direitos stalker da imagem da reclamante ao tirar fotos sem autorização a envolvia em supostas traições para prejudicar seu casamento.
>
> Dessa forma, além de toda a repercussão no ambiente laboral, haja vista que a prova oral disse que todos os funcionários tinham conhecimento, atentou o Sr. Gabriel contra a honra da reclamante e a fidelidade do matrimônio que ela estabeleceu com seu cônjuge, o que se mostra ainda mais perverso. (...)
>
> Com base nos critérios acima descritos, acrescidos da razoabilidade e proporcionalidade, entendo por bem elevar a indenização por danos morais para R$10.000,00.

Portanto, é fato que o *stalking* vem ganhando notoriedade no mundo jurídico, mormente no Direito do Trabalho, com intuito de minimizar os prejuízos da vítima, através da reparação material e/ou moral e de modo a repreender o agressor, para que não mais cometa atitudes inadequadas.

8. Medida estratégica de combate ao *Stalking*

Um dos grandes desafios para o desenvolvimento de intervenções organizacionais é o convencimento das estruturas de comando quanto à aceitação de medida estratégica de combate com o tema stalking e cyberstalking. Há um receio de que, ao tratar abertamente do tema, situações de assédio aparecerão ou, ainda, a abordagem pode ser entendida como o reconhecimento

de ocorrência de casos e das responsabilidades por parte da empresa. (SOBOLL, 2017, p. 33).

Entendemos que esta postura de não aceitação corrobore ainda mais para que a respectiva violência perpetue na clandestinidade.

Entre as possibilidades de medidas de caráter de ação transformadora, que além de combater o stalking, no sentido de coibir tal prática penosa às vítimas, ainda vai mitigar a judicialização contra a empresa.

Nesse sentido, Soboll sugere estratégias de sensibilização, regulamentação e gerenciamento: a sensibilização pode ser feita por cartilhas, palestras, vídeos, eventos, cursos e capacitação técnica; a regulamentação através de leis e normas, códigos de ética ou de conduta, previsão de medidas disciplinares e divulgação do posicionamento organizacional; e o gerenciamento, com diagnóstico contextualizado, apoio aos envolvidos, gestão das informações, consultoria interna e ouvidoria.

Reforçamos que se deve evidenciar os dispositivos legais que implicam a responsabilização das instituições pelos casos de stalking, inclusive em ambiente digital, já definido anteriormente como cyberstalking, daí a necessidade de prevenir e combater o problema: todas as organizações, sem exceção, precisam instruir seus integrantes a respeito desta forma de violência cada vez mais insidiosa e danosa. De facto, cabe às empresas privadas, assim como aos órgãos públicos, a prevenção e o gerenciamento dos casos, mesmo que se trate de assédio interpessoal.

As várias formas de estratégias sugeridas servirão como uma referência formal e institucional que vão orientar a conduta profissional interna e externa de todos os colaboradores. Desta forma, é fundamental que todos os colaboradores estejam cientes das ações transformadoras, compreendam sua importância e apliquem em suas atividades profissionais, dentro e fora das dependências da corporação.

As condutas contrárias a este Código levam à aplicação de medidas disciplinares, que podem incluir o término da relação de trabalho. Buscamos a prática de ações e procedimentos respaldados por leis e não exceções.

1.1. Código de ética e conduta no combate ao stalking inclusive em ambiente digital

Assim sendo, com o objetivo de coibir a prática de condutas de stalking, inclusive no ambiente digital, destacamos a seguir os itens necessários que deverão constar no Código de Ética e Conduta como ação de transformação, no combate ao stalking e cyberstalking.

1.1.1. Respeito às leis

Todo colaborador e estagiário é responsável e tem o compromisso de conhecer e respeitar as leis e normas vigentes aplicáveis às suas atividades, bem como os procedimentos internos da empresa.

A empresa promove o cumprimento de todas as leis municipais, estaduais, federais e internacionais vigentes e aplicáveis ao seu negócio e nos contratos e convênios estabelecidos com o Poder Público e às normas coletivas aplicáveis, e respeitam as prescrições morais, de forma a assegurar relações transparentes, justas e profissionais.

1.1.2. Desenvolvimento e oportunidade profissional

A empresa contribui para a empregabilidade do colaborador e o estimula na busca de seu autodesenvolvimento, oferecendo, a todos, igualdade de oportunidade de desenvolvimento e ascensão profissional, com base no esforço pessoal, mérito, desempenho e competências alcançadas e aderência aos valores.

1.1.3. Meio ambiente, saúde e segurança física e digital

A empresa tem o compromisso de proteger o meio ambiente, a saúde e a segurança física e digital de seus colaboradores e se esforça para proporcionar um ambiente de trabalho seguro e saudável evitando impactos desfavoráveis e danosos ao meio ambiente e nas comunidades onde opera, devendo o colaborador zelar por tal compromisso. Devemos, ainda, nos empenhar em cumprir as leis ambientais, manter um ambiente de trabalho seguro e prevenir acidentes de trabalho.

1.1.4. Assédio moral ou sexual

Fica terminantemente proibida a prática de assédio moral ou sexual, inclusive em ambiente digital, como o WhatsApp corporativo, Mídias sociais corporativas, e-mail, intranet, tanto entre colaboradores de quaisquer níveis hierárquicos, quanto entre estes e o público externo com o qual a Empresa se relaciona: clientes, fornecedores, prestadores de serviço, órgãos públicos e imprensa.

1.1.5. Gestão participativa, inclusive em ambiente digital

A Empresa proporciona um ambiente favorável, com canais de diálogo e participação, de forma que o colaborador possa, efetivamente, contribuir para a gestão da empresa.

1.1.6. Diversidade

Todos os colaboradores, independentemente da posição hierárquica, assumem o compromisso de respeitar a diversidade, inclusive em ambiente digital, exercendo suas funções baseados no comportamento ético, sem preconceito de origem, raça, religião, sexo, cor, idade, altura, peso, aparência física ou quaisquer outras formas de discriminação, na forma preconizada em legislação vigente sobretudo a Lei Geral de Proteção de dados.

9. Conclusão

Do exposto, pode-se concluir que o *stalking* tem se tornado cada vez mais comum e tem ganhado relevância no âmbito judicial, com a criação de mecanismos e legislações específicas, visando a proteção do ofendido e a punição do agressor, seja através de condenações em indenizações por danos morais e materiais, seja através de medidas disciplinares no âmbito do trabalho e até mesmo através de condenações criminais.

É fato que as pessoas precisam despertar a consciência e entender que a conduta reiterada, repetitiva e desagradável de perseguição não é normal e precisa ser imediatamente freada, a fim de evitar maiores danos à vítima, além daqueles já suportados pelo assédio persistente.

Importante destacar que a vítima, embora receosa quanto à intimidação que lhe impõe o *stalker*, tem direitos assegurados e precisa se valer das medidas judiciais aplicáveis a cada caso, como modo de repreender o agressor e se proteger.

Na esfera laboral, em que pese o constrangimento causado, a Justiça do Trabalho tem entendido que casos de *stalking* são passiveis de condenação e merecem atenção, inclusive como meio corretivo de condutas semelhantes.

Com a criminalização do *stalking* possivelmente haverá um maior despertar de conscientização, seja das vítimas (para se assegurarem de que podem e devem denunciar o agressor), seja do agressor (para que avalie suas condutas e as cesse, antes de sofrer uma condenação).

Finalmente, o desenvolvimento de estratégias de sensibilização, o respeito a regulamentação e gerenciamento por meio de códigos de ética ou de conduta, com previsão de medidas disciplinares e divulgação do posicionamento organizacional favorável as ações de combate ao *Stalking*, e o gerenciamento, com diagnóstico contextualizado, apoio aos envolvidos, gestão das informações,

consultoria interna e ouvidoria, contribuirão no sentido de coibir a prática da *stalking* e *cyberstalking.*

Bibliografia

AMIKY, Luciana Gerbovic. Stalking. Disponível em https://tede2.pucsp.br/bitstream/handle/6555/1/Luciana%20Gerbovic%20Amiky.pdf. Acesso em fevereiro/2021.

BLANCO, Enderson. Como identificar o assédio persistente (stalking)? Riscos para as vítimas e solução recomendada. Disponível em https://www.advogadocriminalemsp.com.br/como-identificar-o-assedio-persistente-stalking-riscos-para-vitima-e-solucao-recomendada/. Acesso em fevereiro/2021.

BOEN, Mariana Tordin e LOPES, Fernanda Luiza. Vitimização por Stalking: um estudo sobre a prevalência em estudantes universitários. Disponível em https://www.scielo.br/scielo.php?pid=S0104-026X2019000200218&script=sci_arttext. Acesso em fevereiro/2021.

BRASIL. Código Civil. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em fevereiro/2021.

BRASIL. Código Penal. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em fevereiro/2021.

BRASIL. Código de Processo Penal. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em fevereiro/2021.

BRASIL. Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em março/2021.

BRASIL. Constituição Federal. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em março/2021.

BRASIL. Lei de Contravenções Penais. Disponível em http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3688.htm. Acesso em março/2021.

BRASIL. Lei Maria da Penha. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11340.htm. Acesso em março/2021.

CABETTE, Eduardo Luiz Santos. "Stalking" ou Assédio por Intrusão e violência contra a mulher. Disponível em https://eduardocabette.jusbrasil.com.br/artigos/264233531/stalking-ou-assediopor-intrusao-e-violencia-contra-a-mulher. Acesso em fevereiro/2021.

FERREIRA, Hádassa Dolores Bonilha. Assédio moral nas relações de trabalho. 2. Ed. Campinas: Russel, 2010.

JESUS, Damásio Evangelista de. Stalking. Disponível em https://jus.com.br/artigos/10846/stalking. Acesso em fevereiro/2021.

JOSÉ FILHO, Wagson Lindolfo. Stalking. Disponível em www.magistradotrabalhista.com.br/2015/10/stalking.html. Acesso em fevereiro/2021.

MARCHESI, Sephora. O *stalking* nos acórdãos da relação de Portugal: a compreensão do fenómeno antes da tipificação. *Configurações*, vol. 16, 2015, pp. 55-74.

MATOS, Marlene; GRANGEIA, Helena; FERREIRA, Célia; AZEVEDO, Vanessa. *Inquérito de Vitimação por Stalking: Relatório de Investigação*. Braga: Grupo de Investigação sobre Stalking em Portugal (GISP), 2011a. Disponível em http://repositorium.sdum.uminho.pt/handle/1822/31235. Acesso em março/2021.

MATOS, Marlene; GRANGEIA, Helena; FERREIRA, Célia; AZEVEDO, Vanessa. Stalking: Boas práticas no apoio à vítima. Manual para profissionais. Violência de Género. Lisboa: Comissão para a Cidadania e Igualdade de Género, 2011b. Disponível em

https://www.researchgate.net/publication/289964761_Stalking_Boas_praticas_no_apoio_a_Vitima_Manual_para_profissionais. Acesso em março/2021.

MOROSO, Diana Isabel de Sousa. O Assédio Laboral: Uma Conduta a Criminalizar? Disponível em http://repositorium.sdum.uminho.pt/handle/1822/50542. Acesso em fevereiro/2021.

NASCIMENTO, Sônia Mascaro. Assédio moral. 2. Ed. São Paulo: Saraiva, 2011.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. Código Civil Comentado. 9 ed. São Paulo: Revista dos Tribunais, 2012, p. 977.

SANTOS, Wanderley Elenilton Gonçalves. Assédio moral, bullying, mobbing e stalking: semelhanças, distinções e consequências jurídicas. Disponível em https://ambitojuridico.com.br/edicoes/revista-96/assedio-moral-bullying-mobbing-e-stalking-semelhancas-distincoes-e-consequencias-juridicas/. Acesso em fevereiro/2021.

SPITZBERG, Brian H. The Tactical Topography of Stalking Victimization and Management. Trauma, Violence, & Abuse, v. 3, n. 4, p. 261-188, out. 2002. Disponível em: https://www.researchgate.net/publication/253018184_The_Tactical_Topography_of_Stalking_Victimization_and_Management. Acesso em fevereiro/2021

SPITZBERG, Brian; CUPACH, William. "The State of the Art of Stalking: Taking Stock of the Emerging Literature". *Aggression and Violent Behavior*, v. 12, n. 1, p. 64-86, 2007. https://www.researchgate.net/publication/222953393_The_State_of_the_Art_of_Stalking_Taking_Stock_of_the_Emerging_Literature. Acesso em fevereiro/2021.

TJADEN, Patricia; THOENNES, Nancy. “Stalking in America: Findings from the National Violence against Women Survey”. *Research in Brief*, p. 1-19, abr. 1998. Disponível em https://www.ojp.gov/ncjrs/virtual-library/abstracts/stalking-america-findings-national-violence-against-women-survey. Acesso em fevereiro/2021.

TRINDADE, Jorge. Manual de psicologia jurídica para operadores do direito. Ed Livraria do Advogado, Porto Alegre: 2008, p. 352-353

VITELLI, Romeo. What is Erotomania? 18 mar. 2012. Disponível em https://drvitelli.typepad.com/providentia/2012/03/loving-too-much.html. Acesso em fevereiro/2021.

SOBOLL, Lis Andrea Pereira, Intervenções em Assédio Moral e Organizacional, Editora Ltr. 2017

WELLER, Michelle; HOPE, Lorraine; SHERIDAN, Lorraine. "Police and Public Perceptions of Stalking: The Role of Prior Victim-Offender Relationship". *Journal of Interpersonal Violence*, v. 28, n. 2, p. 320-339, set. 2012. Disponível em https://journals.sagepub.com/doi/10.1177/0886260512454718. Acesso em fevereiro/2021.

_____. Dicas para se proteger dos stalkers virtuais. Disponível em **https://www.kaspersky.com.br/resource-center/threats/how-to-avoid-cyberstalking**. Acesso em março/2021.

LEI Nº 14.132, DE 31 DE MARÇO DE 2021, Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14132.htm

PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - *"SCHREMS II"*

CATARINA CONDE NOGUEIRA *

* Mestranda em segurança da informação e direito ciberespaço.

RESUMO

A uniformização da proteção dos direitos fundamentais dos cidadãos europeus, na transferência dos seus dados pessoais entre a União Europeia e os Estados Unidos da América, representa um desafio na era digital. Na tentativa de garantir um nível de proteção adequado na transferência transatlântica destes dados, a 12 de julho de 2016, a Comissão Europeia estabeleceu a Decisão de Adequação (UE) 2016/1250, mais conhecida como Privacy Shield UE-EUA. Apesar de terem subsistido dúvidas quanto à sua compatibilidade com os requisitos do RGPD, o Privacy Shield esteve em vigor até 16 de julho de 2020, data em que o Tribunal de Justiça da União Europeia declarou inválida a Decisão de Adequação 2016/1250, na decisão que ficou conhecida como Schrems II, a qual veio originar um novo panorama na transferência de dados pessoais para países terceiros.

Palavras-Chave: RGPD; Transferência de dados pessoais para países terceiros; Proteção de dados pessoais; *Privacy-Shield* UE-EUA; *Schrems* II.

ABSTRACT

Ensuring a standardized protection of the European citizens' fundamental rights, when transferring their personal data between the European Union and the United States, represents a challenge in the digital age. To ensure an adequate level of protection in the transatlantic transfer of these data, on 12th July 2016, the European Commission established the Adequacy Decision (EU) 2016/1250, more widely known as the EU-US Privacy Shield. Although there were some doubts regarding its compatibility with the GDPR's requirements, the Privacy Shield was in force until 16th July 2020, when the Court of Justice of the European Union declared the Adequacy Decision 2016/1250 invalid, in the decision known as Schrems II, leading to a new approach for personal data transfer to third countries.

Keywords: Personal data transfer to third countries; Data protection; Privacy-Shield UE-EUA; Schrems II.

1. Introdução

Nos últimos dois anos, mais precisamente desde a implementação do Regulamento Geral de Proteção de Dados (RGPD), a 25 de maio de 2018, tem existido um maior interesse e uma preocupação crescente, tanto por parte dos cidadãos como das empresas, no que diz respeito à privacidade e à proteção dos dados pessoais, bem como a aspiração notória da União Europeia (UE) em afirmar-se como uma referência na proteção jurídica dos titulares de dados.

O Regulamento (UE) n.º 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e à livre circulação desses dados, de 27 de abril de 2016, veio reforçar os direitos fundamentais dos cidadãos da UE na era digital e, de certa forma, minimizar a fragmentação que existia. Este Regulamento Geral de Proteção de Dados aplica-se ao tratamento de dados pessoais efetuado no âmbito das atividades de empresas ou entidades com sucursais estabelecidas na UE, independentemente do local onde os dados são efetivamente processados, bem como ao tratamento de dados pessoais de titulares residentes na UE, efetuado por empresas constituídas fora da UE que ofereçam bens ou serviços a esses titulares ou qualquer tratamento relacionado com o controlo do comportamento destes[1].

No novo mundo virtual, a informação tende a circular sem constrangimentos espaciais, fruto do avanço tecnológico, do qual beneficiam não só os cidadãos, mas também as empresas. Atualmente, a transação de dados pessoais integra as atividades diárias das empresas em todos os setores da economia, tratando-se de uma tendência em crescimento, pelo que a entrada em vigor do RGPD trouxe novas preocupações a todas as empresas que, no âmbito do seu negócio, transferem dados pessoais[2].

1 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.
2 Jesus, I. O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito? 72

Note-se que, de acordo com o Capítulo V do RGPD, relativo às transferências de dados pessoais para países terceiros ou organizações internacionais, o Artigo 45.º "Transferências com base numa decisão de adequação" estabelece que a transferência de dados pessoais é possível, se a Comissão Europeia tiver decidido que o país terceiro ou a organização internacional em causa assegura um nível de proteção adequado. Nestes moldes, a transferência não exige autorização específica. O Artigo 46.º "Transferências sujeitas a garantias adequadas" acrescenta que, caso não tenha sido tomada qualquer decisão nos termos do Artigo 45.º, n.º 3, os responsáveis pelo tratamento ou os subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional, se estes tiverem apresentado garantias adequadas e na condição dos titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.[3]

Resumindo, quando são transferidos dados pessoais para fora da UE, a proteção assegurada pelo RGPD deve manter-se. Assim, pautados pelo nível de exigência que a aplicação do RGPD trouxe, no que concerne à proteção de dados pessoais, e na ausência da decisão de adequação da Comissão Europeia, vários países passaram a adotar medidas idênticas de forma a alcançar a desejada *compliance* que permitisse a continuidade e o crescimento dos seus negócios. Por exemplo, o Brasil adotou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, a qual apresenta semelhanças evidentes ao RGPD, tendo entrado recentemente em vigor, mais precisamente a 18 de setembro de 2020[4]. Outro exemplo a considerar, trata-se da primeira lei do Quénia relativa à proteção de dados pessoais, o *Data Protection Act*, com entrada em vigor a novembro de 2019, o qual, uma vez mais, vai ao encontro dos requisitos do RGPD, no que concerne à recolha, partilha e armazenamento de dados pessoais[5].

A uniformização do nível de proteção dos direitos fundamentais dos cidadãos europeus, na transferência dos seus dados pessoais entre a UE e os Estados Unidos da América (EUA), foco do presente trabalho, representa, sem

3 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 61-62.
4 Governo do Brasil - Ministério da Defesa. Lei Geral de Proteção de Dados – LGPD.
5 Okwara, E. Kenya takes important step toward in data protection.

dúvida, um desafio na era digital. Na tentativa de garantir um nível de proteção adequado, a 12 de julho de 2016, foi tomada a decisão de adequação do *Privacy Shield* UE-EUA. O *Privacy Shield* foi, então, o sistema que, desde 1 de agosto de 2016, procurou garantir *compliance* com os requisitos de proteção de dados pessoais, suportando, assim, o comércio transatlântico destes dados[6], apesar de terem subsistido dúvidas quanto à sua compatibilidade com os requisitos do RGPD, conforme opinião publicada pela Autoridade Europeia para a Proteção de Dados a 30 de maio de 2016.[7] Recentemente, a 16 de julho de 2020, o Tribunal de Justiça da União Europeia (TJUE) declarou inválida a Decisão 2016/1250, relativa à adequação do nível de proteção assegurado pelo *Privacy Shield*, na decisão que ficou conhecida como *Schrems* II, a qual veio corroborar com o cenário de incompatibilidade[8]. Esta decisão é especialmente relevante para o futuro dos fluxos internacionais de dados, ao abrigo dos mecanismos de transferência estabelecidos no RGPD, tendo originado um novo panorama na transação de dados pessoais.

6 Privacy Shield Framework. Privacy Shield Program Overview.
7 Autoridade europeia para a Proteção de Dados. Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision.
8 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.

2. Privacy-Shield UE-EUA

2.1 Breve Enquadramento

Antes da implementação do *Privacy Shield* em 2016, vigoravam, desde o ano 2000, os princípios de privacidade do *Safe Harbor* estabelecidos na Decisão 2000/520[9], até serem considerados incompatíveis com o direito da UE pelo Tribunal de Justiça no acórdão *Schrems* I (cujos acontecimentos serão explicados no terceiro capítulo do presente trabalho)[10].

No que diz respeito ao enquadramento legal da Decisão *Safe Harbor*, esta teve como base a Diretiva da Comissão Europeia 95/46, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. À data já era reconhecida a necessidade de existir fluxos de dados pessoais além-fronteiras, no âmbito do desenvolvimento do comércio internacional. Essas transferências de dados para países terceiros seriam possíveis desde que estes garantissem um nível de proteção adequado, em função das circunstâncias associadas à transferência em causa, e que caso o país terceiro não oferecesse um nível de proteção adequado, a transferência dos dados pessoais deveria, então, ser proibida[11]. Neste sentido, deu-se a negociação entre a UE e os EUA relativamente aos princípios do *Safe Harbor*, a qual foi conduzida pela Comissão Europeia e pelo Departamento de Comércio dos EUA, com acompanhamento técnico do Grupo de Trabalho do Artigo 29.º[12](estabelecido precisamente no artigo 29.º da Diretiva da Comissão Europeia 95/46, o qual foi substituído pelo *European Data Protection Board* (EDPB) aquando da publicação do RGPD).

9 Comissão europeia, Decisão 2000/520 relativa ao nível de proteção assegurado pelos princípios de 'porto seguro' e pelas questões e pelas respetivas FAQ emitidas pelo *Department of Commerce* dos Estados Unidos da América, de 26 de julho de 2000.
10 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão *Schrems*: 93.
11 Comissão europeia, "Decisão da Comissão nos termos da Diretiva 95/46/CE, relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América", de 26 de julho de 2000.
12 Comissão Nacional de Proteção de Dados, Parecer n.º 14/2000.

A Decisão *Safe Harbor* estabelecia os seguintes princípios: princípio de aviso, da escolha, da re-transferência, da segurança, da integridade dos dados, do acesso e da aplicação. Estes princípios eram de aplicação territorial nos EUA e a decisão do seu cumprimento era voluntária, assente na autocertificação das empresas, que teriam de agir em conformidade com os princípios definidos de forma a obterem e manterem os benefícios do *Safe Harbor* e poderem declará-los publicamente[13].

Sumariamente, a decisão de adequação do *Safe Harbor* foi anulada pelas seguintes razões: a sua aplicação, por parte das empresas dos EUA, não garantia um nível de proteção de dados pessoais semelhante ao existente e exigido pela UE; as autoridades norte-americanas não estavam vinculadas a esta Decisão; e, por fim, os dados pessoais de cidadãos europeus podiam, então, ser objeto de tratamento incompatível e desproporcional por partes destas autoridades[14].

Assim, tornou-se premente a revisão do sistema que estabelecia os princípios de privacidade na transferência de dados UE-EUA, na perspetiva do avanço tecnológico e consequente aumento exponencial do fluxo de dados verificado, de forma a garantir um nível de proteção adequado dos dados pessoais e respetivos titulares[15]. Com a elaboração do *Privacy Shield* procurou-se preencher as lacunas do sistema anteriormente em vigor, aumentando o nível de exigência quanto às obrigações das empresas com sede nos EUA, bem como quanto às garantias de supervisão e ainda clarificando o vínculo das autoridades norte-americanas a esta Decisão.

2.2 Caraterização, Âmbito e Princípios

O *Privacy Shield* UE-EUA trata-se de uma *framework* concebida pelo Departamento de Comércio dos EUA, em conjunto com a Comissão Europeia, com o intuito de fornecer às empresas, de ambos os lados do oceano Atlântico,

13 Comissão Nacional de Proteção de Dados, Parecer n.º 17/2000.
14 Raposo, Sá Miranda & Associados, Safe Harbor: Perguntas e Respostas.
15 Comissão europeia, Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema 'porto seguro' na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, de 27 de novembro de 2013: 3.

um mecanismo fiável para cumprir os requisitos de proteção de dados pessoais, aquando da sua transferência da UE para empresas com sede nos EUA, garantindo, assim, que os cidadãos da UE continuem a beneficiar de medidas de proteção adequadas. Esta *framework* baseia-se num sistema de autocertificação, cujo processo será explicado com maior detalhe mais à frente neste trabalho, através do qual as empresas dos EUA assumem o compromisso de estabelecer e cumprir os princípios de privacidade definidos[16]. Assim, o *Privacy Shield* veio trazer novas obrigações que reforçaram a transparência no tratamento dos dados pessoais e facilitaram o exercício dos direitos dos titulares de dados, através da informação obrigatória aos mesmos relativamente às políticas das empresas, no que concerne à proteção de dados pessoais, bem como dos meios existentes para os titulares poderem reagir face ao tratamento dos seus dados pessoais[17].

A *Privacy Shield framework* encontra-se dividida em três capítulos, sendo o primeiro intitulado de "*Overview*", no qual, como o próprio nome indica, são definidos os contornos gerais do programa, assim como o âmbito da certificação segundo o mesmo. No Capítulo II, *"EU-U.S. Privacy Shield Principles*", são definidos os princípios para a proteção dos dados pessoais, os quais procuram garantir o nível de proteção adequado, aplicável a qualquer titular de dados da UE cujos dados sejam transferidos para os EUA, a saber [18]:

1. *Notice*
2. *Choice*
3. *Accountability for Onward Transfer*
4. *Security*
5. *Data Integrity and Purpose Limitation*
6. *Access*
7. *Recourse, Enforcement and Liability*

16 Comissão europeia, "Decisão de execução da Comissão número 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho", de 12 de julho de 2016: 3-4.
17 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 106-107.
18 U.S. Department of Commerce. EU-U.S. Privacy Shield Framework Principles.

O primeiro princípio para a proteção dos dados pessoais, "*Notice*", traduz-se na obrigação por parte empresas certificadas de fornecerem informações chave relacionadas com o processamento de dados pessoais aos respetivos titulares, tais como a categoria dos dados recolhidos, a finalidade do tratamento, os direitos dos titulares de dados, entre outros. O segundo princípio, "*Choice*", confere aos titulares dos dados o direito de se oporem ao tratamento, por exemplo quando se verifica uma alteração na finalidade do tratamento que seja compatível com a finalidade inicial. No entanto, este princípio não afeta a proibição dos tratamentos incompatíveis. O princípio seguinte, "*Accountability for Onward Transfer*", estabelece que qualquer transferência ulterior, ou seja, qualquer transferência de dados pessoais de uma empresa para um responsável pelo tratamento ou um subcontratante, independentemente de este se encontrar nos EUA ou num país terceiro (fora dos EUA e/ou da UE), só é possível para fins específicos e limitados. Na ocorrência destas transferências, deve ser garantido o mesmo nível de proteção acautelado pelos princípios do *Privacy Shield*. O princípio "*Security*" estabelece que as empresas que processam dados pessoais devem implementar medidas de segurança adequadas, as quais devem ter em consideração os riscos relacionados com o processamento em si e com a categoria de dados processados. No que concerne ao princípio "*Data Integrity and Purpose Limitation*", os dados pessoais devem ser exatos, completos, fiáveis e atuais, bem como limitados ao que é realmente relevante para o propósito do tratamento definido. De acordo com este princípio, os dados pessoais só podem ser conservados enquanto a sua utilização esteja conforme a finalidade do tratamento, no entanto, esta obrigação não impede as empresas aderentes ao *Privacy Shield* de continuarem a tratar os dados durante um período mais longo, caso esse tratamento sirva uma finalidade específica, tal como a análise estatística, o jornalismo ou o arquivamento no interesse público. Com o princípio "*Access"* fica então estabelecido que os titulares dos dados têm o direito de obter a confirmação, por parte das empresas, de que os seus dados pessoais estão a ser processados, bem como o direito a que estes lhes sejam comunicados sem demora injustificada. Para além disto, os titulares de dados devem poder alterar ou eliminar informações pessoais sempre que estas estejam incorretas ou tenham sido tratadas em violação dos princípios. Por último, o princípio *"Recourse, Enforcement and Liability"* determina que as empresas certificadas devem

proporcionar mecanismos que assegurem a conformidade com os sete princípios do *Privacy Shield* e também formas de recurso para todos os titulares, cujos dados pessoais tenham sido tratados de modo não conforme[19].

No Capítulo III, *"EU-U.S. Privacy Shield Supplemental Principles*" foram ainda incluídos alguns princípios suplementares, os quais vêm complementar os princípios anteriormente referidos, acrescentando ainda algumas obrigações às empresas certificadas, como por exemplo a obrigatoriedade de verificação da adequação das práticas de privacidade exigidas pelo *Privacy Shield*, quer através de autoavaliação quer de revisões com recurso a entidades externas[20].

Assim, os princípios de privacidade definidos no *Privacy Shield* foram considerados adequados pela Comissão Europeia, na medida em que, no seu conjunto, assegurariam um nível de proteção dos dados pessoais equivalente ao nível assegurado pelo RGPD e, portanto, as empresas dos EUA certificadas também iriam garantir um nível de proteção adequado dos dados pessoais transferidos da UE. Nestes moldes, o *Privacy Shield* viria, então, impedir o acesso indiscriminado aos dados dos cidadãos europeus e a vigilância generalizada dos utilizadores.

À luz deste acordo, o Departamento do Comércio dos EUA foi eleito como a entidade responsável pela monitorização das empresas certificadas, de forma a assegurar que as condições previstas no *Privacy Shield*, nomeadamente a aplicação eficaz dos princípios e as obrigações de transparência no tratamento, fossem cumpridas.

De referir ainda a criação, por parte do governo dos EUA, de um novo mecanismo de supervisão da ingerência da segurança nacional, nomeadamente o Mediador para o *Privacy Shield*, para tratar de eventuais queixas colocadas por

19 Comissão europeia, Decisão de execução da Comissão número 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2016: 4-6.
20 Privacy Shield Framework. 7. Verification.

autoridades de controlo nacionais da UE, em nome dos titulares dos dados no que diz respeito à prática de espionagem nos EUA[21].

2.3 Autocertificação de Empresas

A adesão ao *Privacy Shield*, por parte de empresas com sede nos EUA, é inteiramente voluntária e pressupõe a sua autocertificação anual através do site do Departamento de Comércio dos EUA. Neste processo anual, as empresas comprometem-se a aderir aos Princípios do *Privacy Shield*, a verificar a conformidade das suas políticas e práticas de privacidade e ainda a cooperar com as autoridades com poder de investigação e execução, nomeadamente a *Federal Trade Comission* (FTC), o *Department of Transportation* (DOT), ou qualquer outro organismo oficial americano, na verificação do cumprimento efetivo dos mesmos[22].

De acordo com o guia disponibilizado no site do *Privacy Shield*[23], para a autocertificação das empresas, deve ser tido em consideração, em primeiro lugar, que apenas as empresas com sede nos EUA e, portanto, sujeitas à jurisdição da FTC ou do DOT, são elegíveis para a participação neste programa. O segundo passo para a autocertificação prende-se com o desenvolvimento de uma política de privacidade em conformidade com os princípios do *Privacy Shield*, a qual deve ser estabelecida antes da submissão da candidatura para a autocertificação. Esta política deve refletir as práticas organizacionais para o processamento de informação, bem como os meios disponibilizados aos titulares de dados, no que diz respeito à utilização e divulgação dos seus dados pessoais. Ainda é exigido a existência de uma declaração do compromisso da empresa com os princípios do *Privacy Shield*, incluindo o *hyperlink* para o site do *Privacy Shield*, quando existir confirmação de que a submissão está completa. De acordo com o princípio "*Recourse, Enforcement and Liability*", as empresas devem também

21 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 107.
22 Privacy Shield Framework. How to join Privacy shield (part 1).
23 Privacy Shield Framework. A Step-by-Step Guide to Self-Certification on the Privacy Shield Website.

identificar o mecanismo de recurso independente a quem irão recorrer para investigar eventuais reclamações, o qual tem de estar forçosamente estabelecido antes da certificação. O mecanismo de recurso independente, cujo estabelecimento é verificado pelo Departamento de Comércio dos EUA antes da certificação, deve estar referido também na política de privacidade da empresa. Em adição aos passos anteriores, as empresas que participam no programa *Privacy Shield* UE-EUA, têm de pagar uma contribuição à *American Arbitration Association* (AAA), baseada na dimensão da organização, podendo situar-se entre os $250 e os $10.000 USD, a qual cobrirá os custos do *Arbitral Fund*[24], conforme previsto no Anexo I, "*Arbitration Mechanism*", do *Privacy Shield*. Este fundo permite financiar julgamentos de eventuais violações das obrigações das empresas certificadas para com os cidadãos europeus. Ainda relativamente aos procedimentos necessários para a autocertificação, as empresas devem garantir que têm um mecanismo de verificação *in place*, que inclua procedimentos de autoavaliação internos ou o recurso a entidades externas, que avaliem o seu nível de conformidade com os princípios do *Privacy Shield*. As empresas devem ainda nomear um responsável, dentro da sua organização, que trate de todas as questões relacionadas com a certificação, nomeadamente reclamações, pedidos de acesso, entre outros, com o compromisso de resposta dentro do prazo máximo de 45 dias. Por último, deve ser paga uma taxa de processamento da candidatura no valor de $375 USD. Portanto, este era o procedimento em vigor anterior à decisão que veio invalidar a adequação do *Privacy Shield*.

24 American Arbitration Association. ICDR-AAA EU-U.S. and/or Swiss-U.S. Privacy Shield Arbitral Fund Contributions.

3. Acórdão C-311/18 - "*SCHREMS II*"

3.1 Contexto Anterior (*Schrems* I) e Principais Considerações

A decisão do Tribunal de Justiça da UE (Acórdão C-311/18), de 16 de julho de 2020, a qual ficou conhecida como *Schrems* II, veio invalidar a adequação do *Privacy Shield* quanto ao nível de proteção por este assegurado, relativamente aos dados pessoais de cidadãos europeus transferidos para os EUA.

Na verdade, este Acórdão do TJUE veio na sequência do Acórdão C-362/14, de 6 de outubro de 2015 (*Schrems* I) relativo à queixa apresentada por *Maximillian Schrems*, um cidadão austríaco, advogado e ativista, fundador da organização sem fins lucrativos NOYB (*none of your business*) - *European Center for Digital Rights*, o qual era utilizador do *Facebook* desde 2008. *M. Schrems* alegou que os seus dados pessoais, à semelhança daquilo que acontece com todos os utilizadores europeus, são, no todo ou em parte, transferidos pela *Facebook Ireland* para servidores pertencentes à *Facebook Inc.*, situados nos EUA, onde são objeto de tratamento [25]. As revelações de *Edward Snowden*, antigo colaborador da *National Security Agency* (NSA), uma agência de segurança pertencente à administração dos EUA, trouxeram a público as práticas de vigilância levadas a cabo pelos serviços secretos dos EUA, os quais recolhiam dados pessoais, de forma generalizada e indiscriminada, através da NSA[26]. *M. Schrems*, por considerar que as revelações de *Snowden* não poderiam ser ignoradas, apresentou queixa à autoridade de controlo de proteção de dados da Irlanda - *Data Protection Commissioner*. Neste sentido, *M. Schrems* pretendia obter a proibição destas transferências de dados pessoais e a investigação das práticas do *Facebook* quanto à recolha dos dados pessoais pelas autoridades dos EUA, na medida em que o direito e as práticas dos EUA não confeririam proteção suficiente aos cidadãos da UE, relativamente ao acesso de dados

25 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18: 1.
26 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 98.

pessoais pelas autoridades públicas[27], incluindo a sua utilização em mecanismos de vigilância em massa desenvolvidos pela NSA, pelo FBI, entre outras entidades [28]. Contudo, o *Data Protection Commissioner* desconsiderou a queixa, alegando falta de fundamento, uma vez que os EUA, de acordo com os princípios do *Safe Harbor*, apresentariam um nível de proteção adequado. Discordando desta abordagem, *M. Schrems* recorreu ao Supremo Tribunal Irlandês, o qual considerou que, apesar de *Schrems* não ter colocado formalmente em causa a validade da Decisão *Safe Harbor*, a sua queixa denunciava, no fundo, a legalidade do regime instituído por essa decisão[29]. Neste sentido, o Supremo Tribunal Irlandês questionou o TJUE, via reenvio prejudicial, relativamente à validade da decisão de adequação do *Safe Harbor*, bem como se esta decisão invalidaria o prosseguimento de uma queixa individual, por parte das autoridades de controlo nacionais, quando existem suspeitas da utilização indevida de dados pessoais.

Esta queixa de *M. Schrems* acabou por levar o TJUE a invalidar a Decisão 2000/520, relativa ao nível de proteção assegurado pelos princípios do *Safe Harbor*, atendendo a que este mecanismo não vinculava as autoridades norte-americanas, prevalecendo o direito dos EUA em caso de conflito com os princípios de privacidade definidos[30]. Para tal, foi imperativo o TJUE esclarecer o significado de "nível de proteção adequado", num cenário pré-RGPD, face aos artigos da Carta dos Direitos Fundamentais da União Europeia, à recente jurisprudência e às normas europeias existentes sobre transferências de dados, tendo sido concluído que deveria ser entendido como "substancialmente equivalente" ao garantido pela União Europeia[31]. No seguimento da queixa, o TJUE esclareceu ainda que as autoridades nacionais de proteção de dados têm o

27 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.
28 Pinheiro, A. Consequências do Acórdão Schrems II.
29Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.
30 Lopes, T. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados: 50.
31 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.

dever de investigar queixas relacionadas com o tratamento de dados pessoais em países terceiros, mesmo quando já existe uma decisão de adequação *in place*.

Ainda na sequência do Acórdão *Schrems* I, o TJUE identificou alguns pontos fulcrais para que a *framework* para a proteção de dados no país terceiro seja equivalente à da UE, nomeadamente: eficácia da *framework*, ou seja, o país terceiro deve garantir a existência de instrumentos jurídicos para a proteção dos direitos fundamentais, que sejam capacitados para responsabilizar e punir eventuais infratores; existência de meios de recurso judicial, disponíveis aos titulares, que garantam uma forma de reação efetiva contra as empresas que executam o tratamento de dados pessoais[32].

Naquele que foi o início do segundo episódio da saga, *M. Schrems* foi convidado a reformular a sua queixa, considerando a anulação do *Safe Harbor*. Nesta queixa, *M. Schrems* manteve a tese de que os EUA não assegurariam uma proteção eficaz dos dados transferidos e solicitou a suspensão ou proibição da transferência UE-EUA dos seus dados pessoais. A *Facebook Ireland*, entretanto, passou a transferir os dados tendo como base as cláusulas de proteção de dados presentes no anexo da Decisão 2010/87[33], relativa a cláusulas contratuais-tipo, as ditas *Standard Contractual Clauses* (SCC), aplicáveis à transferência de dados pessoais da UE para subcontratantes estabelecidos em países terceiros. A autoridade de controlo irlandesa, ao considerar que o tratamento da queixa de *M. Schrems* estaria dependente da validade da Decisão 2010/87, iniciou um processo para que o Supremo Tribunal Irlandês submetesse ao TJUE um pedido de decisão prejudicial[34]. De notar que, durante o período que sucedeu o início deste processo, a Comissão Europeia emitiu a Decisão 2016/1250, relativa ao nível de proteção assegurado pelo *Privacy Shield* UE-EUA, revogou a Diretiva 95/46, relativa à proteção das pessoas singulares no que diz respeito ao

32 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 98.
33 Comissão europeia, Decisão de execução da Comissão número 2010/87, a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016.
34 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.

tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995, a qual foi substituída pelo Regulamento (UE) 2016/679 e ainda emitiu a Decisão 2016/2297 que alterou as Decisões 2001/497 e 2010/87, relativas às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros.

O TJUE foi questionado quanto à aplicabilidade do RGPD nas transferências de dados pessoais com base nas cláusulas da Decisão 2010/87, quanto ao nível de exigência do RGPD, no que diz respeito à proteção de dados pessoais transferidos para países terceiros e quanto às obrigações das autoridades de controlo neste contexto. Assim, surgiu a questão da validade tanto da Decisão 2010/87 como da Decisão 2016/1250.

O Tribunal de Justiça entendeu que o RGPD é aplicável a qualquer transferência de dados pessoais, no âmbito de uma atividade comercial, efetuada por um operador económico estabelecido num Estado-Membro para um outro operador estabelecido num país terceiro, independentemente de eventuais tratamentos posteriores a que os dados possam ser submetidos no país de destino, incluindo para efeitos de segurança pública, de defesa e de segurança do Estado pelas autoridades do país terceiro em causa[35]. Relativamente ao nível de proteção dos dados pessoais transferidos para países terceiros, importa referir que o artigo 46.º do RGPD "Transferências sujeitas a garantias adequadas", prevê que, no nº 1, se não tiver sido tomada uma decisão de adequação, os responsáveis pelo tratamento só podem transferir dados pessoais para um país terceiro "se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes" e que, de acordo com o nº 2 (alínea c), essas garantias podem resultar de "cláusulas-tipo de proteção" elaboradas pela Comissão. Em suma, o TJUE afirmou que os requisitos do RGPD sobre direitos oponíveis, garantias adequadas e medidas jurídicas eficazes devem ser aplicados de forma que os titulares, cujos dados são transferidos para um país terceiro com base em SCC, possam beneficiar de um nível de proteção equivalente ao assegurado na UE. Assim, o nível de proteção

35 Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020.

adequado deve ser avaliado tendo em conta as estipulações contratuais acordadas entre o exportador (UE) e o destinatário dos dados pessoais (país terceiro), bem como os elementos pertinentes do sistema jurídico do país terceiro em causa[36]. Por último, quanto às obrigações das autoridades de controlo, no contexto da transferência de dados pessoais para países terceiros, o TJUE declarou que, em conformidade com o artigo 58.º ("Poderes"), nº 2 do RGPD, interpretado em conjunto com o artigo 8.º ("Direito à proteção de dados pessoais"), da Carta dos Direitos Fundamentais da União Europeia, o respeito das exigências, que o direito fundamental à proteção de dados pessoais implica, está sujeito ao controlo de autoridades independentes, pelo que estas autoridades devem agir de forma a assegurar a correta aplicação deste regulamento. Portanto, a não ser que exista uma decisão de adequação adotada pela Comissão, as autoridades de controlo estão incumbidas de suspender, ou até mesmo proibir, as transferências de dados para países terceiros sempre que considerarem que as SCC não são ou não podem ser respeitadas pelo país terceiro em causa e quando a proteção adequada dos dados transferidos, exigida pela UE, não pode ser assegurada por outros meios, no caso do próprio exportador não ter posto termo à transferência[37].

No decorrer deste processo, a validade da Decisão 2010/87 foi examinada, considerando a sua versão atual resultante da Decisão de Execução 2016/2297. De acordo com o TJUE, a sua validade não pode ser colocada em causa, uma vez que as SCC estabelecidas na Decisão não vinculam as autoridades do país terceiro por terem um caráter contratual. No entanto, a sua validade está inteiramente dependente da existência de mecanismos efetivos que garantam o respeito do nível de proteção adequado, exigido pelo direito da UE, e que possibilitem a suspensão/proibição da transferência de dados pessoais, com base nessas SCC, em caso de violação das mesmas ou na impossibilidade do seu cumprimento. O TJUE manifestou que esta Decisão prevê tais mecanismos, os quais advêm da imposição, tanto ao exportador como ao destinatário dos dados, de levar a cabo esta verificação prévia, bem como à obrigação do destinatário

36 Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.
37 Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.

informar o exportador sempre que se verifique a impossibilidade de cumprir o estabelecido nas SCC, pertencendo ao exportador o dever da suspensão da transferência e/ou da rescisão do contrato[38].

Por último, a validade da Decisão 2016/1250, relativa ao nível de proteção assegurado pelo *Privacy Shield*, foi também alvo de investigação face aos requisitos do RGPD, lidos à luz das disposições da Carta dos Direitos Fundamentais da União Europeia. O TJUE pronunciou que, à semelhança da Decisão *Safe Harbor*, a Decisão *Privacy Shield* não estabelecia as garantias necessárias contra a ingerência das autoridades de informação norte-americanas no exercício dos direitos fundamentais dos titulares, cujos dados são transferidos para este país terceiro, relativos ao respeito da vida privada, à proteção dos dados pessoais e à proteção jurisdicional efetiva. Deste modo, a regulamentação interna dos EUA, no que diz respeito ao acesso e utilização dos dados pessoais provenientes da UE pelas autoridades públicas americanas, resulta numa grave fragilidade na proteção adequada dos dados e seus titulares, pelo que a exigência do nível de proteção "equivalente" ao garantido na UE não é satisfeita, na medida em que os programas de vigilância levados a cabo com base nessa regulamentação não são limitados ao estritamente necessário. Acrescentou ainda que a regulamentação interna dos EUA, apesar de incluir exigências para as autoridades americanas aquando da implementação dos ditos programas de *surveillance*, não confere aos titulares dos dados direitos oponíveis às autoridades americanas nos tribunais[39].

Ainda no que diz respeito à imposição de proteção jurisdicional, o TJUE declarou que o mecanismo de mediação previsto no *Privacy Shield*, contrariamente ao que a Comissão considerou aquando da sua decisão de adequação, não oferece aos titulares uma via de recurso num órgão que apresente garantias proporcionais às exigidas pelo direito da UE, as quais sejam capazes não só de assegurar a independência do mediador previsto, mas também a

38 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18: 3.
39 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.

existência de normas que o habilitem a adotar decisões vinculativas para os serviços de informações americanos[40].

Considerando os motivos apresentados, o TJUE concluiu que, à luz da Carta dos Direitos Fundamentais da União Europeia, tendo por base os artigos 7.º, 8.º e 52.º (direito à vida privada, direito à proteção de dados pessoais e âmbito e interpretação dos direitos fundamentais, respetivamente), a validade da Decisão 2010/87 não é afetada, no entanto, declarou inválida a Decisão 2016/1250, uma vez que o *Privacy Shield*, à semelhança do *Safe Harbor*, consagrava o primado das exigências relativas à segurança nacional, ao interesse público e ao respeito da legislação americana, possibilitando assim ingerências nos direitos fundamentais dos cidadãos europeus, cujos dados são transferidos para os EUA[41].

3.2 Análise Crítica Geral

Atualmente, as empresas, independentemente do seu setor de atuação, seriam incapazes de fazer negócio ou participar no comércio internacional sem terem a capacidade de transferir dados além-fronteiras. O comércio global da UE está intimamente ligado ao fluxo transfronteiriço de dados, sendo as SCC o principal instrumento legal e o mecanismo mais amplamente utilizado para a transferência de dados pessoais para países terceiros, sendo, portanto, essenciais para a economia global[42].

A conclusão do TJUE relativamente à adequação das SCC para garantir contratualmente um nível de proteção equivalente dos dados transferidos para um país terceiro pretendeu, no fundo, não gerar um limbo jurídico. Esta decisão é, de certa forma, ambígua na medida em que a necessidade de garantir o cumprimento de medidas adequadas para proteger os dados pessoais, de acordo com os artigos 45.º ("Transferências com base numa decisão de adequação") e

40 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.
41 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.
42 Digital Europe. An early analysis of Schrems II – key questions and possible ways forward.

46.º ("Transferências sujeitas a garantias adequadas") do RGPD, aplica-se tanto às decisões de adequação da Comissão Europeia como a cláusulas-tipo. Ora, se o *Privacy Shield* foi considerado inválido com base na incompatibilidade entre o direito da UE e a legislação de segurança norte-americana, seria expectável que as SCC estabelecidas para regular a transferência de dados precisamente para os EUA também teriam a mesma consequência jurídica. Portanto, perante este cenário, não é fácil compreender que as SCC não estejam também sujeitas a escrutínio por parte da Comissão, no que diz respeito à adequação da proteção oferecida na transferência de dados pessoais para um país terceiro, por não se dirigirem concretamente a um Estado, tendo o TJUE interpretado o RGPD de forma a atribuir às autoridades de controlo a competência desta verificação[43].

No fundo, o TJUE decidiu em conformidade com a jurisprudência dos últimos anos, a qual assenta numa posição firme a favor da proteção de dados pessoais, cabendo à lei governar a tecnologia e não o contrário, pelo que as empresas e outras partes interessadas devem encontrar soluções que permitam oferecer a proteção adequada dos dados pessoais exigida na UE[44]. Por exemplo, em 2017, o Tribunal emitiu o Parecer 1/15, projeto de acordo entre o Canadá e a UE - transferência dos dados dos registos de identificação dos passageiros aéreos, no qual se opôs à entrada em vigor do Acórdão, insistindo no estabelecimento de regras rigorosas quanto à implementação concreta das leis de vigilância[45]. Em 2016, nos acórdãos *Tele2 Sverige* e *Tom Watson*, o Tribunal impôs limitações aos regimes de retenção de dados pessoais decididos pelos governos da UE e, em 2014, no Acórdão *Digital Rights Ireland*, o TJUE declarou inválida a Diretiva de retenção de dados[46].

Na Decisão *Schrems* II, o TJUE concluiu que, para as SCC serem válidas, os responsáveis pelo tratamento e os subcontratantes, em colaboração com o país destinatário dos dados pessoais, devem realizar uma avaliação da adequação do

43Pinheiro, A. Consequências do Acórdão Schrems II.
44 Christakis, T. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1).
45 Parecer do Tribunal de Justiça 1/15 de 26 de julho de 2017, Projeto de acordo entre o Canadá e a União Europeia.
46 Christakis, T. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1).

sistema jurídico do país terceiro, com base nos requisitos do artigo 45.º do RGPD e tendo em conta as circunstâncias específicas da transferência. Sempre que esta avaliação não demonstrar a garantia de uma proteção eficaz, em particular devido ao risco de acesso indevido dos dados pessoais por parte das autoridades públicas do país terceiro, o responsável pelo tratamento ou o subcontratante só poderão considerar as SCC aplicáveis às suas transferências de dados se existir a possibilidade de estas adotarem medidas adicionais que possam colmatar o risco de inadequação do país terceiro, reforçando, assim, a proteção dos dados transferidos[47]. Contudo, na ausência de uma decisão de adequação propriamente dita, a determinação sobre se uma lei de vigilância de um país terceiro satisfaz ou não as salvaguardas necessárias, no que diz respeito à proteção de dados pessoais está longe de ser simples, indo muito além das regulares diligências entre fornecedores e clientes.

A necessidade de realizar avaliações relativas à adequação dos países terceiros, caso a caso, além de representar um encargo adicional para os responsáveis pelo tratamento e respetivos subcontratantes, os quais muitas vezes são empresas com recursos limitados, sendo cerca de 65% PME's ou *startups*[48], a autoridade e o dever destes decidirem sobre a adequação dos regimes de segurança nacional de outros países é, no mínimo, discutível por não ser uma tarefa tipicamente esperada de empresas privadas.

Outra questão que se coloca, no que diz respeito às avaliações exigidas da adequação do sistema jurídico do país terceiro, prende-se com a possibilidade de existirem avaliações diferentes entre empresas, originando soluções contraditórias relativamente às SCC, as quais apenas poderiam ser resolvidas pelas autoridades de controlo, que, por sua vez, também poderiam apresentar avaliações contraditórias, sendo necessária uma interpretação uniforme entre as autoridades de controlo nacionais da UE[49].

47 Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020.
48 Moniz, G. Schrems II – a saga da proteção de dados pessoais continua.
49 Digital Europe. An early analysis of Schrems II – key questions and possible ways forward.

A 11 de novembro de 2020, a *European Data Protection Board* (EDPB) emitiu a Recomendação 1/2020, relativamente às medidas adicionais para complementar as ferramentas de transferência de dados pessoais, incluindo as SCC, de forma a garantir *compliance* com o nível de proteção exigida na UE. Nesta recomendação, a qual foi emitida precisamente na sequência da Decisão *Schrems* II, a EDPB aconselha as empresas exportadoras de dados, em primeiro lugar, a conhecer bem as suas transferências, estando cientes de onde circulam os dados e da adequação e relevância dos mesmos, em relação ao propósito pelo qual são transferidos e processados no país terceiro, seguindo-se um *roadmap*, dirigido às empresas, para aplicação do princípio da responsabilidade nas transferências de dados pessoais, incluindo recomendações para a verificação da adequação da ferramenta de transferência em uso, para a avaliação da proteção assegurada no país terceiro e para a adoção de medidas suplementares[50]. Ao ler as recomendações relativas à adoção de medidas suplementares, ficamos com a sensação de que qualquer transferência de dados pessoais da UE para países terceiros que não beneficiem de uma decisão de adequação da Comissão, será difícil. A EDPB, no Anexo 2, fornece uma lista não exaustiva de tais medidas, incluindo medidas técnicas, contratuais e organizativas, e afirma que, nos casos em que nenhuma medida suplementar possa corrigir as deficiências identificadas, as transferências deverão ser interrompidas. No que diz respeito às medidas técnicas, a encriptação dos dados pessoais é a medida a destacar pela EDPB como a principal técnica para exportar dados de forma segura (uma vez que impossibilita o acesso aos dados propriamente ditos no país destinatário), sobre a qual são feitas várias recomendações relativas à sua aplicação, incluindo a necessidade de encriptação antes da transferência de dados, a resiliência da encriptação obrigatória face à criptanálise pelas autoridades públicas dos países terceiros, a implementação impecável do algoritmo de encriptação em si, a imposição de manter as chaves de encriptação na UE, entre outras[51]. Portanto, após as empresas terem conduzido as avaliações da adequação do sistema jurídico do país terceiro e implementado as medidas suplementares

50 EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
51 EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

imprescindíveis à transferência de dados pessoais, sempre que tal seja possível, ainda têm que documentar este processo e submeter o pedido de autorização, sempre que exigido pelo mecanismo de transferência escolhido e reavaliar a sua abordagem regularmente. Claramente, a orientação emitida pela EDPB é complexa, representando um enorme desafio para as empresas da UE, as quais estão perante uma tarefa quase impossível - encontrar soluções que permitam manter o padrão de proteção de dados da UE, independentemente do país destinatário, num mundo global em que os direitos, as leis e as normas divergem consideravelmente[52].

52 Fennessy, C. A breakdown of EDPB's recommendations for data transfers post-'Schrems II'.

4. Reflexões Finais

O Acórdão proferido pelo TJUE (C-311/18, "*Schrems* II") veio consolidar a importância de manter um nível de proteção elevado no que concerne aos dados pessoais transferidos da UE para países terceiros, abordando, de forma genérica, a questão do acesso a dados pessoais pelo governo e autoridades públicas por parte de qualquer país terceiro. Na verdade, a decisão do caso *Schrems* II vai bastante além do *Schrems* I, na medida em que o primeiro episódio apenas invalida os princípios de privacidade do *Safe Harbor*, para a transferência de dados UE-EUA, enquanto que no *Schrems* II, além da decisão de adequação *Privacy Shield* UE-EUA ter sido invalidada, o TJUE insistiu que todos os intervenientes relevantes devem assegurar que o *standard* para a proteção de dados pessoais da UE é mantido e aplicado quando se recorre a outros meios legais para a transferência de dados, que não decisões de adequação.

Com o caso *Schrems* II fica claro que as SCC são atualmente a alternativa a considerar no que diz respeito à transferência de dados pessoais para os países que não beneficiem de uma decisão de adequação, pelo que as empresas devem focar-se no estabelecimento de SCC personalizadas, as quais garantam a manutenção do nível de proteção dos dados pessoais assegurada pelo RGPD aquando da sua transferência para um país terceiro, não se limitando, portanto, a utilizar um *template* contratual. No entanto, uma garantia contratual não deixa de ser insuficiente se a lei do país terceiro exigir ou permitir o acesso a dados pessoais em contradição com os requisitos do RGPD. Deste modo, os Responsáveis pelo Tratamento, sob o controlo das Autoridades de Proteção de Dados, ficam incumbidos de assegurar a eficácia das SCC na prática, o que, por si só, representa um desafio considerável para as empresas, as quais têm de levar a cabo *a priori* uma avaliação para determinar se o país terceiro oferece ou não garantias legais equivalentes às da UE. Escusado será dizer que esta avaliação pode terminar com as transferências de dados para um número importante de Estados, nomeadamente a China e a Rússia, cujos sistemas jurídicos oferecem substancialmente menos garantias do que os EUA em relação ao acesso dos dados por autoridades públicas e governamentais.

Assim, este Acórdão trouxe várias incertezas quanto à base jurídica para as transferências internacionais de dados pessoais, incluindo inseguranças relativas à perspetiva de uma versão 3.0 da decisão de adequação *Safe Harbor*, para além de também levantar questões relativamente às decisões de adequação em vigor com outros países terceiros.

Em adição, veio ainda revelar algumas inseguranças relacionadas com a avaliação dos países terceiros quanto à garantia de proteção adequada dos dados pessoais e seus titulares, uma vez que, até à data do Acórdão, a responsabilidade desta avaliação era centralizada na Comissão Europeia, tendo havido uma viragem para a descentralização desta autoridade no sentido de colocar este processo sob o controlo das autoridades nacionais competentes. Ora, se a própria Comissão Europeia com todo o seu conhecimento e recursos ao dispor, provou estar errada duas vezes consecutivas em relação a tais avaliações (*Safe Harbor* e *Privacy Shield*), coloca-se a questão pertinente de como poderiam as empresas da UE ter um melhor desempenho nesta tarefa.

O estabelecimento de uma regulação transfronteiriça para a proteção de dados pessoais é um processo bastante complexo pela necessidade de satisfazer, por um lado, a preocupação de salvaguardar a liberdade do desenvolvimento empresarial e, simultaneamente, garantir um nível de proteção adequado dos dados pessoais e seus titulares, e, por outro, assegurar a proteção da segurança nacional e ainda manter uma relação diplomática e comercial com os países terceiros, especialmente com aqueles que são as grandes potências internacionais.

Não existindo uma solução ideal, as decisões de adequação da Comissão Europeia, durante vários anos, foram a principal base legal para a transferência de dados além-fronteiras, no entanto, a postura exigente do TJUE vem insistir na afirmação efetiva do direito fundamental à proteção de dados. Poder-se-ia esperar que o *Schrems* II surtisse o efeito desejado de promover a convergência dos *standards* de proteção de dados a nível internacional, como forma de facilitar o fluxo de dados e, consequentemente, o comércio. Esta saga jurisprudencial

gerou pressão nos países terceiros, por verem o tráfico de dados dificultado, estando a UE a tentar, de certa forma, afirmar-se como um "regulador" para a transferência de dados pessoais a nível internacional. Outro dado importante, será observar como as autoridades de controlo nacionais irão agir perante este Acórdão quando ainda não houve tempo suficiente para se tirar conclusões definitivas. O tema da proteção de dados está longe de estar esgotado e a divergência do entendimento relativo à privacidade é tão vincado que garantir um nível de proteção eficaz, independentemente do local para onde os dados pessoais viajam, constitui um enorme desafio sem solução definitiva num horizonte próximo.

Bibliografia

Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=pt [Consultado a 08/11/2020].

Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B7696A55E724D9CD6BAC0B89552911FD?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=13263774 [Consultado a 15/11/2020].

American Arbitration Association. ICDR-AAA EU-U.S. and/or Swiss-U.S. Privacy Shield Arbitral Fund Contributions. [Online]. Disponível em: https://go.adr.org/privacyshieldfund.html [Consultado a 01/11/2020].

Autoridade europeia para a Proteção de Dados. Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, de 30 de maio de 2016. [Online]. Disponível em: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf [Consultado a 01/11/2020].

Christakis, T. 2020. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1). [Online]. Disponível em: https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ [Consultado a 22/11/2020].

Comissão europeia, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema 'porto seguro' na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE", de 27 de novembro de 2013, p. 3. [Online] Disponível em: http://eur-lex.europa.eu/legal-

content/PT/TXT/PDF/?uri=CELEX:52013DC0847&qid=1488287495250&from=PT> [Consultado a 10/11/2020].

Comissão europeia, "Decisão 2000/520 relativa ao nível de proteção assegurado pelos princípios de 'porto seguro' e pelas questões e pelas respectivas FAQ emitidas pelo Department of Commerce dos Estados Unidos da América", de 26 de julho de 2000. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT [Consultado a 10/11/2020].

Comissão europeia, "Decisão de execução da Comissão número 2010/87, a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho", de 5 de fevereiro de 2010. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0087&from=PT Consultado a 13/11/2020].

Comissão europeia, "Decisão de execução da Comissão número 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho", de 12 de julho de 2016, p. 3-6. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016D1250&from=PT. [Consultado a 05/11/2020].

Comissão europeia, "Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América", de 26 de julho de 2000. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT [Consultado a 15/11/2020].

Comissão Nacional de Proteção de Dados, Parecer n.º 14/2000 [Online]. Disponível em: https://www.cnpd.pt/home/decisoes/2000/htm/par/par014-00.htm [Consultado a 15/11/2020].

Comissão Nacional de Proteção de Dados, Parecer n.º 17/2000 [Online]. Disponível em: https://www.cnpd.pt/home/decisoes/2000/htm/par/par017-00.htm [Consultado a 15/11/2020].

Digital Europe. 2020. An early analysis of Schrems II – key questions and possible ways forward [Online]. Disponível em: https://www.digitaleurope.org/resources/an-early-analysis-of-schrems-ii-key-questions-and-possible-ways-forward/ [Consultado a 21/11/2020].

EDPB. 2020. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020. [Online]. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [Consultado a 22/11/2020].

Fennessy, C. 2020. A breakdown of EDPB's recommendations for data transfers post-'Schrems II'. [Online]. Disponível em: https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/ [Consultado a 22/11/2020].

Governo do Brasil - Ministério da Defesa. 2020. Lei Geral de Proteção de Dados – LGPD [Online]. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd [Consultado a 31/10/2020].

Jesus, I. 2018. O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito? *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 05/11/2020].

Lopes, T. 2018. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados: 50. *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 10/11/2020].

Moniz, G. 2020. Schrems II – a saga da proteção de dados pessoais continua. *In* Observador [Online]. Disponível em: https://observador.pt/opiniao/schrems-ii-a-saga-da-protecao-de-dados-pessoais-continua/ [Consultado a 21/11/2020].

Okwara, E. 2020. Kenya takes important step toward in data protection. [Online]. Disponível em: https://iapp.org/news/a/kenya-takes-important-step-forward-in-data-protection/ [Consultado a 31/10/2020].

Parecer do Tribunal de Justiça 1/15 de 26 de julho de 2017, Projeto de acordo entre o Canadá e a União Europeia - Transferência dos dados dos registos de identificação dos passageiros aéreos da União para o Canadá. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62015CG0001&from=IT [Consultado a 22/11/2020].

Pinheiro, A. 2020. Consequências do Acórdão Schrems II. [Online]. Disponível em: https://asousapinheiro.com/2020/08/21/consequencias-do-acordao-schrems-ii/ [Consultado a 14/11/2020].

Pires, M. 2018. Algumas considerações sobre a compatibilidade do sistema de *Privacy Shield* com o direito da União Europeia à luz do acórdão Schrems. *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 05/11/2020].

Privacy Shield Framework. How to join Privacy shield (part 1). [Online]. Disponível em: https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 [Consultado a 01/11/2020].

Privacy Shield Framework. Privacy Shield Program Overview. [Online]. Disponível em: https://www.privacyshield.gov/Program-Overview [Consultado a 01/11/2020].

Privacy Shield Framework. A Step-by-Step Guide to Self-Certification on the Privacy Shield Website. [Online]. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000 79DJ [Consultado a 01/11/2020].

Privacy Shield Framework. 7. Verification. [Online]. Disponível em: https://www.privacyshield.gov/article?id=7-Verification [Consultado a 08/11/2020].

Raposo, Sá Miranda & Associados. 2015. *Safe Harbor*: Perguntas e Respostas. [Online]. Disponível em: https://www.pra.pt/site/assets/files/1222/safe_harbor_nota_informativa.pdf [Consultado a 15/11/2020].

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT [Consultado a 31/10/2020].

Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B7696A55E724 D9CD6BAC0B89552911FD?text=&docid=221826&pageIndex=0&doclang=P T&mode=lst&dir=&occ=first&part=1&cid=13263774 [Consultado a 15/11/2020].

Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18. [Online]. Disponível em:

https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf [Consultado a 08/11/2020].

U.S. Department of Commerce. EU-U.S. Privacy Shield Framework Principles. [Online]. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [Consultado a 01/11/2020].

CYBERLAW by CIJIC

AQUISIÇÃO DE DADOS DE TRÁFEGO EM PROCESSO PENAL: *"PESCA À LINHA"* vs. *"PESCA DE ARRASTÃO"*

EMANUEL MONIZ VIVEIROS *

* Mestrando Segurança informação e direito ciberespaço.

RESUMO

A recolha de metadados por operadoras de telecomunicações pode ser extremamente útil para identificar criminosos e proteger as vítimas.

No entanto, com o crescimento contínuo de utilizadores de smartphones e a cada vez maior e consequente pegada digital deixada para trás, a recolha e o acesso a metadados por entidades judiciais deve ser feita de forma (precisa) que obste a que dados de utilizadores sem qualquer conexão com o caso concreto sejam "*vazados*" e divulgados ao público.

Palavras-Chave telecomunicações; dados de tráfego; suspeito; crime roubo agravado.

ABSTRACT

The collection of metadata from telecom operators may prove extremely useful to identify criminals and to protect victims.

However, with the continuous growth of smartphone users worldwide and consequent ever-increasing digital footprint left behind, the collection of metadata must be done in such a (precise) way that prevents data from users without any connection to the specific case to be "dumped" and disclosed to the public.

Keywords: telecommunications; traffic data; metadata; suspect; theft crime.

1. Introdução

O presente trabalho visa analisar o Acórdão do Tribunal da Relação de Lisboa, datado de 22/06/2016, proferido no âmbito do processo n.º 48/16.3PBCSC-A.L1-9, cujo Relator foi Sérgio Calheiros da Gama, o qual pode ser consultado em www.dgsi.pt.[1]

O referido Acórdão do Tribunal da Relação de Lisboa incide sobre um recurso penal interposto pelo Ministério Público, porquanto pretendia que fossem oficiadas as operadoras de telecomunicações, para que procedessem à junção aos autos de dados de tráfego[2] recolhidos numa determinada área geográfica e num determinado período temporal.

Em causa estava a investigação de um crime de roubo e posse de arma proibida, ocorrido numa residência sita em Cascais, no dia 9 de janeiro de 2016, pelas 02h:30m. Na residência assaltada estavam três pessoas, tendo uma delas sido golpeada com recurso a uma arma branca.

As vítimas conseguiram descrever que se tratavam de quatro indivíduos, todos do sexo masculino, sendo que três deles mediam cerca de 1,80m e o quarto entre 1,85m/1,90m, este de pele morena, com determinado sotaque, com o braço esquerdo com uma tatuagem, uma peruca com rastas no cabelo e olhos cor de mel.

Na posse desta descrição dos presumíveis autores do crime foram feitos exames periciais ao local em que os factos ocorreram e ainda uma análise ao relatórios de alguns assaltos ocorridos em momento anterior e posterior à data dos factos da ocorrência em investigação nos autos ora em análise, da qual resultou uma forte convicção de que alguns dos ilícitos identificados, atenta a forma de atuação dos indivíduos, composição e características identificadas semelhantes, terem sido os mesmos os seus autores.

1 Último acesso em 10 de janeiro de 2021.
2 Faremos referência a "*metadados*" e "*dados de tráfego*" enquanto sinónimos.

Com este cenário em pano de fundo e sem mais qualquer prova que permitisse identificar os autores do roubo, veio o Ministério Público requerer que fossem oficiadas as operadoras de telecomunicações no sentido de juntar aos autos os metadados de dezanove estações base em Cascais, os quais permitiriam encontrar coincidências entre os titulares dos números móveis e as descrições que dos assaltantes foram feitas.

O Juiz de Instrução indeferiu o requerimento apresentado pelo Ministério Público, tendo este interposto o recurso que ora se analisa.

A análise

O Recurso ora em análise enquadra-se nos autos de inquérito do processo n.º 48/16.3PBCSC, que correu termos no Departamento Central de Investigação e Ação Penal – 3.ª Secção, do Tribunal Judicial da Comarca de Lisboa Oeste – Cascais.

No requerimento apresentado, o Ministério Público requereu que fossem oficiadas as operadoras de telecomunicações MEO, Vodafone e NOS, para "*que aquelas operadoras juntem aos autos a "listagem - em suporte digital e formato Excel, contendo todos os dados de tráfego - registos completos das comunicações efetuadas e recebidas nas [19] BTS (infra identificadas), detalhes das comunicações eventos de rede (lixo eletrónico), com indicação da hora e com indicação dos números chamados e chamadores, incluindo as mensagens de texto, duração e hora das chamadas e localização celular - relativos aos cartões SIM que operaram entre as 01h45 do dia [9 de Janeiro de 2016] e as 02h30 do dia 9 de Janeiro de 2016, quanto às antenas que se identificam (...)*".

O Requerimento acabado de elencar enquadra-se nos autos de inquérito e visa investigar factos ocorridos em 9 de janeiro de 2016, pelas 02h:30m, no interior de uma residência, sita em Cascais, os quais são suscetíveis de *"de integrar, em abstracto, a prática de crime de* ***roubo agravado****, previsto e punido pelo disposto no artigo 210.º, n.ºs 1 e 2, alínea b) do Código Penal (atento o disposto no artigo 204.º, n.º 2, alínea f) do*

Código Penal), e um crime de ***detenção de arma proibida****, previsto e punido pelo artigo 86.º, do Regime Jurídico das armas e suas munições."*[3]

Nos referidos autos, e após realizadas "*diversas diligências foi possível trazer aos autos uma descrição física dos autores (quatro indivíduos, do sexo masculino: três deles mediam cerca de 1,80m e o quarto entre 1,85m/1,90m, este de pele morena, com sotaque, com o braço esquerdo com uma tatuagem, trazia uma peruca com rastas no cabelo e tinha olhos cor de mel) (…)*"

Perante estas características dos suspeitos, o Ministério Público requereu ao Juiz de Instrução que, "*ao abrigo do disposto nos artigos 10.º e 7.º, n.ºs 2 e 3 da Lei n.º 32/2008, de 17 de Julho, fossem as operadoras de telemóveis oficiadas para que remetessem relação de todos os cartões SIM e respetivos IMEI que tenham estado presentes e ativos nas células que se discriminaram (dados de tráfego armazenados), com menção da respetiva localização celular, para o curto período temporal entre a 01h45m e as 02h30m do dia 9 de Janeiro de 2016.*"

De forma a enquadrar e justificar o seu pedido, o Ministério Público sublinhou a "***gravidade*** *do crime cometido*" e a *"****indispensabilidade*** *da diligência, com menção de que outras não se vislumbravam que pudessem alcançar o duplo objetivo de localização e identificação dos autores dos factos e de que a listagem remetida seria sujeita à respetiva análise, sendo única e exclusivamente junta aos autos a informação pertinente para a investigação."*[4]

Aqui chegados, temos que o Ministério Público baseou o seu requerimento no disposto na Lei n.º 32/2008, de 17 de julho, sem fazer referência aos artigos 187.º a 189.º do Código de Processo Penal,[5] nem qualquer referência à Lei 109/2009, de 15 de setembro (Lei do Cibercrime), máxime artigo 14.º, nem tão pouco qualquer referência ao disposto no artigo 4.º da Lei nº 41/2004, de 18 de agosto, referente à proteção de dados pessoais e privacidade nas telecomunicações.

3 Sublinhado e negrito nossos.
4 Sublinhado e negrito nossos.
5 O Tribunal da Relação de Lisboa entende que o regime constante dos artigos 187.º a 189 do Código de Processo Penal é aplicável a "*"dados sobre a localização celular", obtidos em tempo real e intercepção das comunicações entre presentes*" enquanto que o âmbito de aplicação da Lei 32/2008 de 17 de julho circunscreve-se aos "*dados que concernem a comunicações relativas ao passado ou seja, arquivadas …*", cf. Acórdão do Tribunal da Relação de Lisboa, processo n.º 1585/16.5PBCSC-A.L1-5, disponível em www.dgsi.pt.

Para mais, vem o Ministério Público requerer dados relativos a dezanove (!) estações base, todas elas sita no centro de Cascais. Ao invés, pensamos que o Ministério Público devia, num primeiro momento, oficiar as operadoras de telecomunicações no sentido de informar qual a estação base que têm instalada mais perto da morada onde se deu o crime. É que os telemóveis tendem sempre a se conectar à estação base com melhor sinal e, em meios urbanos, atenta a diversidade de obstáculos para a propagação do sinal de rádio, o melhor sinal costuma ser o sinal que está a menor distância.

Este pequeno passo prévio, o qual não passaria sequer pelo crivo do Juiz de Instrução, permitiria reduzir de dezanove para apenas três estações base e, consequentemente, reduzir drasticamente o número de dados a transmitir ao processo, o que, como veremos adiante, poderia conduzir a um diferente desfecho do presente caso.

Aqui chegados, e considerando a sua importância na análise do presente, transcreve-se de seguida os principais fundamentos do Recurso apresentado pelo Ministério Público:

> *" (...)*
>
> *e) Em primeiro lugar, sempre se dirá que terá de se atender ao teor da diligência requerida, que mais não é do que uma listagem de números de telemóvel e de IMEI (correspondendo tal à identificação do equipamento utilizado) - uma vez que diferentes cartões podem encontrar-se associados ao mesmo aparelho - que accionaram antenas determinadas num período temporal restrito, reduzido a quarenta e cinco minutos de madrugada, e da qual não consta qualquer conteúdo das operações realizadas.*
>
> *f) Em segundo lugar, sempre se dirá que, nos termos do disposto nos artigos 125.º e 126.º do Código de Processo Penal apenas são admissíveis todas as provas que não forem proibidas por lei, devendo aqui entender-se à constante no artigo 262.º do referido diploma legal e aos princípios de idoneidade, necessidade e proporcionalidade – "estas três vertentes são requisitos intrínsecos de toda a medida processual restritiva de direitos fundamentais e exigíveis, tanto no momento da sua previsão pelo legislador, como na sua aplicação prática" (in Código de Processo Penal Comentado, Henriques Gaspar e outros, 2014, ALMEDINA). Ora, não*

sendo prova proibida, aferida a pertinência da diligência e mostrando-se a mesma respeitadora dos princípios indicados, teria de ser a mesma deferida.

g) Em terceiro lugar, certo é que a decisão judicial de que ora se recorre não procede a qualquer apreciação do requerido, fazendo aplicar as normas previstas no Código de Processo Penal, afastando o regime previsto na Lei n.º 32/2008, de 17 de Julho, o qual é invocado na promoção que antecede, por se entender que constitui o aplicável à recolha de prova eletrónica por localização celular conservada, sem enunciar qualquer fundamento para tal.

h) Mais se afirme, que dúvidas inexistem quanto à gravidade do ilícito em investigação - o qual constitui, em nosso entender, no crime que maior intranquilidade gera na sociedade, em face do modo aleatório coma as vítimas são escolhidas, a indiferença pelas mesmas e pela sua vida e a violência gratuita utilizada na sua consumação - e que a informação que se pretende recolher - listagem de números e IMEI que activaram um número determinado de antenas, num período de apenas 45 minutos (curto, refira-se) -, visando alcançar a dupla finalidade de localização e identificação dos suspeitos, alcançará efeitos úteis perante a possibilidade de comparação da mesma com a de outras investigações em curso e nas quais são descritos modos de atuação similares praticados por indivíduos cujas características em tudo se assemelham às dos descritos nos presentes autos.

i) Por último, e parecendo resultar da decisão ora recorrida que a rejeição se funda na falta de identificação cabal de quem é o suspeito, sempre se dirá que, nos termos da definição constante do artigo 1.º, alínea e) do Código de Processo Penal, o mesmo é "toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou nele participou ou se prepara para participar", não se exigindo que o mesmo seja uma pessoa determinada ou identificada, mas apenas que estejamos perante "uma pessoa concreta, com determinadas características, ainda que não devidamente apurada a respectiva identidade e sobre a qual existam indícios de que cometeu ou se prepara

para cometer um crime" (Acórdão do Tribunal da Relação de Évora de 10 de Julho de 2014, Processo n.º 36/14.4GDEVR-A.E1).

j) A noção de suspeito avançada no despacho de que ora se recorre, não tendo correspondência na lei, constitui uma limitação excessiva do normativo, produzindo, no limite, a ineficácia do meio de prova em causa em todos os casos em que o agente do crime não se mostra cabalmente identificado.

k) Mais se acrescente que, em todo o caso, os dados obtidos, atenta a forma como solicitados, não violariam a privacidade de qualquer cidadão. Por um lado, porque a listagem remetida apenas conteria uma lista dos números/IMEI que acederam, em determinado dia e hora, a uma determinada antena, sem qualquer informação sobre o conteúdo dessa operação e, por outro lado, porquanto a informação que seria junta aos autos respeitaria única e exclusivamente aos 'suspeitos' e 'intermediários' (artigo 10.º da Lei n.º 32/2008, de 17 de Julho) em estrito cumprimento dos princípios constitucionais erigidos nos artigos 26.º, n.º 1, 34.º, n.º 1 e 18, n.ºs 2 e 3 da Constituição da República Portuguesa.

l) O indeferimento da diligência, uma vez que se mostram preenchidos todos os requisitos legais – gravidade e indispensabilidade – e se aferem protegidos os princípios da idoneidade, necessidade e proporcionalidade (além do mais, em face do modo como a informação seria remetida e o conteúdo a verter para os autos) vai contra as próprias finalidades da investigação criminal, nos termos do constante no artigo 262.º, n.º 1 do Código de Processo Penal.

m) Pelo que, com o despacho judicial proferido a M.ma Juiz de Instrução violou o disposto nos artigos 125.º, 126.º, 262.º, n.º 1 do Código de Processo Penal, bem como os artigos 10.º e 7.º, n.ºs 2 e 3 da Lei n.º 32/2008, de 17 de Julho e procedeu a uma interpretação restritiva e violadora da definição constante do artigo 1.º, alínea e) do Código de Processo Penal, devendo o mesmo ser revogado e substituído por outro que determine a remessa dos elementos solicitados, nos termos requeridos na promoção que o antecede.

Pelo exposto, deve o presente recurso merecer provimento, revogando-se a decisão judicial recorrida e substituindo-a por outra que determine a remessa aos autos das informações solicitadas nos termos e para os efeitos referidos, só assim se fazendo a esperada e costumada JUSTIÇA"[6]

Admitido o Recurso, o Procurador Geral Adjunto no Tribunal da Relação de Lisboa após visto legal, aderindo integralmente aos argumentos apresentados, acrescentando, ainda, que "*para identificar suspeitos, a diligência pretendida mostra-se essencial (para não dizer que, a nosso ver, única), sendo que, para esse fim, a mesma é legal e admissível, como muito bem se explica nos Acs. da RL lavrados no Proc.º 833/l0.0PAMTJ-A.Ll-5 em 18-01-2011 e 97/10.5PJAMD-A.Ll-5 em 11-01-2011, bem como no da RE lavrado no Proc.º 98/08.3PESTB.E1 em 12-04-2011 e no da RC lavrado no Proc.º 174/12.8JACBR.C1 em 22-10-2014, todos eles acessíveis em www.dgsi.pt.""*

Em face do requerimento apresentado, foi delimitado o âmbito do recurso "*à questão de saber se se mostram reunidos os pressupostos legais para que seja ordenado às operadoras de telemóveis identificadas pelo MP na promoção que veio a ser indeferida pelo despacho ora recorrido que forneçam aos autos os dados de tráfego armazenados e de localização celular ali indicados.*"

Delimitado o **objeto do Recurso**, o Tribunal da Relação de Lisboa procedeu à sua análise, a qual se transcreve:

"No caso em apreço, visa-se chegar à identificação dos autores dos crimes através da análise de coincidências que venham a ser encontradas nos dados obtidos através de localização celular nos locais da prática dos fatos e no período temporal em que estes ocorreram.

Nos termos do disposto no art. 187.°, nº 2 do CPP aplicável "ex vi" do art. 189.° do mesmo Código, a obtenção e junção de dados sobre a

6 Sublinhado nosso.

localização celular só podem ser ordenadas ou autorizadas em relação às pessoas referidas no nº 4 do mesmo artigo.

Por sua vez, as pessoas referidas no nº 4 do art. 187.º do CPP são os suspeitos, arguidos, pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de arguido ou de vítima do crime.

Acresce que a noção processual de suspeito é delimitada pela al. e) do art. 1.º do CPP, sendo "toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar".

No requerimento em apreço, invoca o Ministério Público que os fatos em investigação nos autos foram praticados por quatro indivíduos do sexo masculino, todos encapuçados e calçando luvas e que os ofendidos não conseguem proceder ao reconhecimento dos autores dos fatos em virtude de estes terem atuado com os rostos cobertos.

Pede a Digna Magistrada do Ministério Público que se ordenasse às operadoras o fornecimento de todos os cartões SIM que estivessem na posse das pessoas que, além do mais, tivessem o seu telefone ligado no dia 9.01.2015, entre as 01h45m e as 02h30m, em várias áreas da localidade de Cascais, como sejam, entre outras: Cascais Praia, Cascais FDD 2Cascais MSC LC 3, Cascais PT 2, Cascais Centro.

Sucede que, partindo do conceito de suspeito que nos é dado no citado art. 1.º, al. e) do CPP, a jurisprudência tem entendido que para o preenchimento da noção de suspeito é necessário que se trate de pessoa concreta, determinável, passível de individualização.

Tal não acontece no caso dos autos em que não foi possível determinar os suspeitos do crime de roubo indiciado por se encontraram com os rostos cobertos e envergavam luvas.

Assim sendo, in casu não existe suspeitos nos termos legalmente exigidos, além do que em face do vastíssimo leque de potenciais visados atento o requerido, entendemos que no caso concreto, o interesse público

em que se traduz o exercício da ação penal não deverá prevalece sobre o interesse subjacente ao sigilo profissional e das comunicações de um leque tão grande de incertos.

Neste sentido, decidiu o Tribunal da Relação de Lisboa de 17.12.2014, disponível in www.dgsi.pt. em cujo sumário consta o seguinte:

"I - A existência de um catálogo de alvos obsta à determinação de escutas telefónicas em processo contra incertos.

II- O legislador pretendeu que a autorização judicial tivesse por referência as conversações mantidas por pessoas concretas, ainda que não seja conhecida a sua identidade civil.

III - São, portanto, inadmissíveis as escutas telefónicas determinadas a grupos de pessoas cujo único traço comum é o de ocuparem habitualmente ou esporadicamente um determinado espaço físico."

E ainda o mesmo Tribunal da Relação de Lisboa (9ª secção) no recente acórdão de 17.12.2015, proferido no processo n.º 848/14.9PFCSC-A.L1, onde consta o seguinte:

"Tal significa que ***a diligência pretendida iria trazer aos autos os dados de tráfego e de localização celular de um número indeterminado de cidadãos, tornando-os alvo de uma investigação na qual não têm a qualidade de suspeitos, com a inerente postergação dos direitos constitucionais à privacidade e reserva da sua vida e à inviolabilidade das comunicações, sem qualquer garantia de efeito útil, ou seja, de que entre eles se encontrassem os autores dos ilícitos, pois que, na verdade, nem é certo que estes tivessem consigo telemóveis pessoais***.

E como bem se salienta no referido acórdão "não estando concretizados alvos determináveis, e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de "suspeitos", ***o deferimento da sua realização iria contra o disposto na al. a) do n° 3 do art. 9.° da Lei n.º 32/2008. de 17-07. para além de não respeitar os princípios da proporcionalidade e***

<u>da adequação cuja observância o n.º 4 desse normativo e o art. 18.º, n.º 2, da CRP impõem."</u>

Nestes termos e atento o expendido, entendemos que o requerido pela Digna Magistrada do Ministério Público carece de fundamento legal.

Termos em que se <u>indefere ao requerido</u>."[7]

Ora, notamos que o artigo 9.º da Lei 32/2008 de 17 de julho admite a transmissão de metadados "*se houver razões para crer que a diligência é indispensável*" (art.º 9, n.º 1).

Contudo, não estando provado nos autos que os autores do crime tinham o telemóvel consigo, parece-nos difícil que o Ministério Público consiga justificar a "indispensabilidade" da diligência requerida (em especial, no tocante à extensão de dados a transmitir ao processo por falta de delimitação).

Para mais, o supra citado artigo 9.º <u>apenas</u> permite a transmissão de dados referentes às pessoas constantes do seu n.º 3, onde efetivamente constam os "suspeitos". Assim, ao requerer uma transmissão de dados de forma tão abrangente, temos que o Ministério Público não teve minimamente em linha de conta o conceito de "suspeito", o qual inclusive tem sido bastante trabalhado na jurisprudência dos Tribunais superiores.

Por fim, mas não menos importante, o n.º 4 do artigo 9.º ora em análise refere que a "*decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade*", o que sempre resultaria do disposto no artigo 18.º, n.º 2 da Constituição da República Portuguesa.

Como é sabido, o princípio da proporcionalidade é analisado tripartidamente: i) adequação; ii) necessidade e iii) proporcionalidade em sentido estrito.

Assim, aplicando um "teste de proporcionalidade" ao requerido pelo Ministério Público, temos que não existe forma de alegar que a diligência requerida é idónea na medida que o Ministério Público não tem elementos para concluir que os autores do crime se encontravam na posse dos seus telemóveis quando o cometeram. Neste caso, ainda que

7 Sublinhado e negrito nossos.

a diligência fosse autorizada e o "arrastão" de dados executado, sempre se poderia chegar a uma situação em que não é possível proceder à identificação dos autores do crime.

Mais a mais, atenta a necessidade de balançar a necessidade da diligência requerida com o direito à privacidade que assiste aos cidadãos, os quais, sem sequer terem qualquer ligação ao processo veriam "despejados" em público dados sobre as suas comunicações, pensamos que a diligência requerida nunca passaria pelo crivo da proporcionalidade em sentido estrito.

Atento o que fica transcrito, coube ao Tribunal da Relação de Lisboa analisar se a Juiz de Instrução junto do Tribunal *a quo* poderia ter deferido a pretensão do Ministério Público e, consequentemente, ordenar as operadoras Vodafone, NOS e MEO, no sentido de estas juntarem aos autos os dados de tráfego armazenados, em relação a 19 *sites*, todos em Cascais.

Aquando da sua análise, o Tribunal da Relação de Lisboa começou por amparar juridicamente a questão que lhe fora colocada com o disposto no artigo 1.º da Lei n.º 32/2008, de 17 de Julho, o qual se transcreve:

> *"1 - A presente lei* ***regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas****, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.*
>
> *2 - A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de*

18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações."[8]

O Tribunal da Relação de Lisboa continua a sua análise, concluindo, previamente, que estando em causa metadados, a sua transmissão deve ser feita com observância do disposto no art. 9.º, n.ºs 1 a 3 da Lei 32/2008 de 17 Julho, o qual dita:

"1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º ***só pode ser autorizada, por despacho fundamentado do juiz de instrução****, se houver razões para crer que a diligência é* ***indispensável*** *para a descoberta da verdade ou que a* ***prova seria, de outra forma, impossível ou muito difícil de obter*** *no âmbito da investigação, detecção e repressão de crimes graves.*

2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 - Só pode ser autorizada a transmissão de dados relativos:

a) Ao ***suspeito*** *ou arguido;*

4 - A decisão judicial de transmitir os dados deve respeitar os ***princípios da adequação, necessidade e proporcionalidade****, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.(...)"*[9]

Do normativo em análise resultam os requisitos necessários para a transmissão de metadados, a saber: i) tenham sido pedido pelo Ministério Público ou pela autoridade de polícia criminal competente; ii) que sirva de suporte à investigação, deteção e repressão de crimes graves; iii) que seja indispensável para a descoberta da verdade, sendo também admissível nos casos em que a prova seria, de outra forma, impossível ou muito difícil de

8 Sublinhado e negrito nossos.
9 Sublinhado e negrito nossos.

obter, e iv) que os dados a transmitir sejam relativos às pessoas elencadas no n.º 3 do artigo 9.º, no caso em análise, referente a meros suspeitos.

Para além dos requisitos ora elencados, manda expressamente o n.º 4 do transcrito artigo 9.º da Lei 32/2008 de 17 de julho que a decisão de transmissão de dados respeite "*os princípios da adequação, necessidade e proporcionalidade*".

Como refere, e bem, o Tribunal da Relação de Lisboa, quando "*estão em causa direitos, liberdades e garantias constitucionalmente protegidos, como o direito à privacidade e reserva da vida privada e familiar e à inviolabilidade das comunicações (cf. arts. 26.º, n.º 1, 34.º, n.º 1 e 18.º, n.ºs 2 e 3, todos da CRP), as respectivas restrições têm de obedecer aos pressupostos materiais da necessidade, adequação e proporcionalidade em sentido restrito, competindo, em primeira linha, ao legislador ordinário assegurar esses pressupostos ao legislar sobre a matéria*".

Prossegue o Acórdão, confirmando que nos autos estava efetivamente em causa "*a investigação de um crime de roubo agravado (em concurso com um crime de detenção de arma proibida), ilícito que se enquadra no conceito de "criminalidade violenta"",* pelo que, nesta sede, confirma que a diligência do Ministério Público visa suportar a investigação, deteção e repressão de crimes graves (artigo 2.º, n.º 1, al. g) da Lei n.º 32/2008 de 17 de julho.

Aqui chegados, vem o Tribunal da Relação de Lisboa enquadrar o requerimento do Ministério Público em face do conceito de "*suspeito*" previsto no artigo 9.º, n.º 3, al. a) da Lei n.º 32/2008 de 17 de Julho, conceito este constante do disposto no artigo 1.º, n.º 1 al. e) do CPP, que define suspeito como sendo "*toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar*".

Na sua análise, o Tribunal da Relação de Lisboa parte da extensa jurisprudência que se debruça sobre o conceito de suspeito, concluindo que:

> *" (...) a jurisprudência tem entendido que para o preenchimento da noção de suspeito não é necessário que seja conhecida a identificação civil da pessoa em concreto relativamente à qual se visa a utilização do meio de obtenção de prova em causa. Contudo, não pode tratar-se de uma*

mera abstracção; ainda que não identificada: é necessário que se trate de pessoa concreta, determinável, passível de individualização.

*Em suma, **a existência de um suspeito**, enquanto interveniente processual, não implica a sua identificação completa, mas **não dispensa a existência de dados factuais com base nos quais possa individualizar-se uma pessoa determinada, não podendo tratar-se apenas de um abstracto agente do crime**. ''*[10]

Prossegue o Tribunal da Relação de Lisboa a sua análise, referindo que a diligência requerida pelo Ministério Público tem a potencialidade de atingir negativamente um número demasiado elevado e incerto de cidadãos, ao invés de tão só permitir identificar os potenciais autores do crime.

Para tal, sem nunca traçar uma fronteira concreta, refere o exemplo hipotético de o assalto, ao invés de se dar em Cascais, "*se dava num "monte alentejano", pequeno e isolado por sua natureza, ou numa casa das muitas aldeias serranas ditas do "xisto", de tal modo despovoadas fruto da emigração, em que nalgumas nem os antigos habitantes aí pernoitam, aí se quedando apenas ocasionalmente dois ou três forasteiros adeptos do turismo rural e de natureza. Ou ainda, um qualquer outro lugar em que a densidade populacional seja baixíssima, como é o caso dos concelhos de Alcoutim ou Mértola, em que o número médio de habitantes por quilómetro quadrado é de cinco (dados do INE/PORDATA com base no último recenseamento geral da população portuguesa, efetuado em 2011).*

Afirmando de seguida que o número de habitantes por quilómetro quadrado em Cascais é muito superior, a rondar os 2.200. Para mais "*Cascais cobre vastas zonas de areal e praia, caso das dunas do Guincho ou da Quinta da Marinha, e de mata e serra, ou praticamente desertas, como sucede com campos de golfe e com toda a área ocupada pelo Autódromo do Estoril, consequentemente, e segundo as regras da experiência comum, o centro da vila de Cascais registará em realidade e obviamente uma densidade populacional muito superior à da totalidade do concelho*.".

"Acresce que, os censos à população só cobrem os cidadãos que residem habitualmente em determinado local e não os que aí tem residências secundárias nem

10 Sublinhado e negrito nossos.

muito menos os turistas nacionais e estrangeiros que ficam alojados nas suas estadas em hotéis e outros alojamentos similares.

Sucede que Cascais, facto que é público e notório, é uma estância turística, cosmopolita, de lazer e jogo, de organização de congressos internacionais e de muitos eventos culturais e promocionais de natureza comercial, atraindo anualmente milhares de pessoas não residentes.

Segundo dados estatísticos divulgados pela Câmara Municipal de Cascais no seu site institucional, em 2014 o setor da hotelaria registou mais de 1,2 milhões de dormidas (1,202.918), sendo que hoje na área metropolitana de Lisboa a atividade turística e o afluxo de estrangeiros é cada vez menos sazonal, estendendo-se ao longo de todo o ano e já não só no período de Verão."

Assim, após elencar localizações geográficas de baixa densidade populacional, onde seria, em abstrato, aceitável deferir o requerido pelo Ministério Público, por tal não implicar uma recolha massiva de dados de terceiros, a par de evidenciar que Cascais tem uma grande densidade populacional, o Tribunal da Relação de Lisboa chega à conclusão que à hora indicada pelo Ministério Público, "*ainda haverá no centro de Cascais muita gente acordada bem como de que o trafego era pedido para 19 (dezanove) antenas das redes telemóvel situadas no Centro de Cascais, não será difícil de calcular em muitos milhares os dados que constariam na tal listagem*", considerando que, ao diferir tal diligência, estaria a permitir um "*verdadeiro arrastão*" de dados, o que não é permitido à luz do direito processual penal vigente, porquanto o Ministério Público deve proceder à recolha de prova "*de forma fina, isto é como na pesca à linha ou, quanto muito, como na pesca de cerco, mas nunca como na pesca de arrastão, em que nem tudo o que vem à rede é peixe*."

Prossegue o Tribunal da Relação de Lisboa, referindo que na pesca por arrastão "*acabam por vir na rede não só peixes, moluscos, crustáceos, etc., de fauna marítima autorizada, mas também lixo (literalmente) e sobretudo e infelizmente, de forma acidental, espécies protegidas e/ou ameaçadas de extinção, desde cetáceos a tartarugas marinhas, igualmente com diligências do tipo da ora requerida pelo Ministério Público viriam porventura às malhas da justiça elementos que quiçá levariam a identificar suspeitos, aqueles que esta se propõe agora com muita dificuldade apurar quem são e seguidamente melhor investigar e perseguir criminalmente, já como arguidos*

constituídos, acusados e/ou pronunciados, levando-os a julgamento em vista da sua condenação, como também viria "lixo", havendo ainda vítimas colaterais, que seriam os milhares de cidadãos que veriam ser violada a sua privacidade, pois, contrariamente ao que pretende fazer crer o recorrente Ministério Público, o facto de se não ficar a conhecer o conteúdo do tráfego não exclui a possibilidade de graves repercussões na vida de um inocente estranho à lide, porquanto o simples facto de uma pessoa ligar para outra, cujos números de telemóvel e de IMEI são revelados, a determinada hora, a partir de certo local e com uma duração de chamada telefónica de X tempo, já está por si só a facultar a terceiros preciosos elementos de referenciação" pelo que o *"Juiz de Instrução enquanto garante dos direitos, liberdades e garantias dos cidadãos, constitucionalmente consagrados, não o pode permitir.*".[11]

Algumas *interjeições* finais

Apresentados os argumentos que sempre conduziriam ao indeferimento do requerido pelo Ministério Público, o Tribunal da Relação de Lisboa prossegue no sentido de evidenciar os perigos da "*pesca por arrastão*" que o Ministério Público pretendia levar avante, dando um exemplo concreto daquilo que presumimos ser, na linguagem empregue pelo Tribunal, "*espécies protegidas*":

> *"No caso concreto ainda nos apercebemos da existência de um honorável cidadão - que presentemente até goza de foro e prerrogativas especiais nesta matéria - que veria com grande e séria probabilidade o seu tráfego de dados do telemóvel figurar na listagem pedida pelo Ministério Público.*
>
> *Trata-se de Sua Excelência o Senhor Presidente da República. Com efeito, o Exmº Professor Doutor RR tinha e continua a ter a sua residência particular, onde assiduamente pernoitará, no centro de Cascais a escassos metros da residência assaltada nos autos, sita na DD (de que constam duas imagens aéreas, de satélite, do google earth a fls. 38 e cinco*

11 Sublinhado e negrito nossos.

fotografias ao nível da rua a fls. 39, todas juntas pelo LPC da PJ) e das antenas de que o Ministério Público pretende o tráfego de dados.

É certo que o Senhor Professor RR só foi eleito, pelos portugueses, para a Presidência da República em 24 de Janeiro de 2016 e só tomou posse no mais alto cargo do Estado a 9 de Março. Todavia, a 9 de Janeiro de 2016, data dos factos sob investigação, ou seja, 15 dias antes da referida eleição, estava-se em plena recta final da campanha eleitoral para as presidenciais, bem se sabendo que o então candidato Marcelo Rebelo de Sousa é pessoa que dorme pouco.

Todos os canais de televisão (RTP, SIC e TVI) deram imagens em directo da sua saída da residência particular no centro de Cascais para Lisboa (sede da campanha em Belém e seguidamente para a Faculdade de Direito da UL) na noite do dia da sua referida eleição após serem conhecidos os resultados.

Tudo isto são factos públicos e notórios, os quais, concatenados com os em apreço nos autos, permitem formular o raciocínio traçado quatro parágrafos acima.

Temos que a referência ao Professor Marcelo Rebelo de Sousa é exemplificativa do perigo a que o deferimento deste tipo de requerimento de prova conduziria.

Pensamos, contudo, que o facto de a recolha de dados pretendida incidir sobre um momento em que o possível "alvo" dessa recolha é mero candidato à Presidência da República não tem relevância jurídica. Admitiríamos o contrário caso o Professor Marcelo fosse, à data, mais do que mero candidato à Presidência. Em todo o caso, pensamos não ser aplicável o disposto no artigo 11.º, n.º 2, al. b) do Código de Processo Penal, o qual prevê que compete ao Presidente do Supremo Tribunal de Justiça, em matéria penal "*autorizar a interceção, a gravação e a transcrição de conversações ou comunicações em que intervenham o Presidente da República ...*".

Aqui chegado, conclui o Acórdão do Tribunal da Relação de Lisboa que o crime em investigação gera na sociedade, tal como refere o Ministério Público, "*a maior intranquilidade*". Contudo, "*a devassa da vida íntima e/ou privada dos cidadãos perante*

as novas tecnologias da comunicação também gera na sociedade atual uma grande intranquilidade", terminando o aresto ora em análise com a negação do provimento do recurso.

CYBERLAW by CIJIC

A PROEMINÊNCIA DA *NET NEUTRALITY* E AS SUAS ADVERSIDADES

EDUARDO SIMÕES BARROS*

* Mestrando em segurança da informação e direito ciberespaço.

RESUMO

Com o atual valor da *internet* e dos seus ativos começam a surgir problemas que pelo facto de colidirem com alguns direitos humanos são de grande relevo. Um dos debates mais acesos nesta medida é o da net neutrality. Este documento apresenta o conceito de *net neutrality*, explica porque a falta dela é tão perigosa para os direitos humanos, perspetiva as partes contra e a favor, analisa algumas soluções que podem ser adotadas e esclarece alguns pontos que aparentam discordantes como o do *Quality of Service* (QoS). Após enquadrada a *net neutrality* são analisadas as abordagens Americana e Europeia que visam solucionar, através de peças legislativas, os problemas inerentes à *net neutrality* (ou à falta dela).

Palavras-Chave: Net neutrality, Direitos humanos, *Quality of Service*, Abordagem Americana à net neutrality, Abordagem Europeia à *net neutrality*.

ABSTRACT

With the current value of the internet and its assets, relevant problems start to emerge since they conflict with some human rights. One of the most heated debates in this regard is the net neutrality. This document presents the concept of net neutrality, explains why the lack of it is so dangerous for human rights, analyzes the prospects for and against, analyzes some solutions that can be adopted and clarifies some points that seem to be discordant like that of the Quality of Service (QoS). After framing the net neutrality, the American and European approaches that aim to solve, through Legislative pieces the problems inherent to the net neutrality (or the lack of it) are analyzed.

Keywords: Net neutrality, Human rights, Quality of Service, American approach to net neutrality, European approach to net neutrality.

1. Introdução

É difícil pensar num aspeto da vida humana que não tenha sido afetado pela *internet*. A *internet* alterou por completo o conceito de aprendizagem e investigação, permitindo um acesso praticamente ilimitado e livre à informação. Facilitou as comunicações, o uso de vários serviços públicos, a forma como se efetuam compras e revolucionou por completo o conceito de trabalho. São infindáveis as oportunidades e os valores que a *internet* ocasionou, não só pelos valores que acrescentou à vida humana, como pelo valor econômico atual dos ativos da *internet*, sendo vista por muitos como o novo petróleo.

Considerando o peso que a *internet* passou a ter na vida do ser humano, é natural que se discutam as liberdades associadas ao uso da mesma, a liberdade de expressão, a liberdade individual ou mesmo se o acesso à *internet* é ou não um direito fundamental. Só por si, o relevo que estes debates têm demonstra a importância e o risco das tecnologias de informação nos tempos que correm. Será lógico então ampliar os direitos fundamentais que constam na constituição portuguesa para o ciberespaço e o acesso ao mesmo?

A *internet* cultiva o direito ao conhecimento e possibilita a um indivíduo o seu próprio desenvolvimento. Aliado a estas caraterísticas, a *internet* permite que o direito à liberdade de expressão seja usado e abusado de uma forma massiva. Esta prática permitiu que muitas organizações criassem livremente a sua iniciativa, havendo mesmo casos em que a gestão da organização é efetuada através de escritórios virtuais, como o caso do *GitLab*, uma das empresas de *software* mais usado no mundo [1].

Em muito a *internet* e as suas propriedades assemelham-se a um espaço físico, com várias propriedades que o próprio não goza. Para a prospeção do ser humano, o acesso à *internet* deve ser um direito fundamental. Apesar de surgirem

1 Disponível em: https://about.gitlab.com/blog/2016/11/17/web-summit-summary/

novos problemas com esta afirmação, nomeadamente a garantia de acesso à mesma, para que a influência da *internet* na vida humana seja colocada de forma realista, a mesma deve ser considerada como um direito fundamental. O ponto 6 do artigo 35 da constituição portuguesa aborda de forma leviana este tema quando refere "*A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional*"[2].

Um dos debates mais acesos do momento é o da *net neutrality* que apesar de ser um tema aparentemente idêntico ao acesso livre à *internet* têm fundamentos diferentes. Entende-se que o conceito de "internet aberta" corresponde às condições de acesso à própria *internet*, em contrapartida, o conceito de *net neutrality* aponta para as práticas de gestão do tráfego. No fundo, o paradigma da *net neutrality* dita que todos os bits de uma comunicação devem ser tratados da mesma forma, não podendo haver manipulação dessa informação, quer seja através do bloqueio, do retardamento ou do acréscimo de condições para o acesso à informação, não importando as circunstâncias, o país de acesso nem o conteúdo que se acede.

Por um lado, os *Internet Service Providers* (ISP), entidades que permitem aos utilizadores o acesso à *internet*, conseguem mais benefícios manipulando o tráfego à sua medida, quer seja privilegiando o tráfego de entidades protocoladas ou privilegiando os seus próprios serviços. Ainda com uma posição análoga, os criadores do serviço que têm como objetivo a satisfação do cliente, estão interessados em ver o seu tráfego ser tratado de forma superior, podendo isto, acidentalmente, levar a uma monopolização da prática de tratamento diferenciado do tráfego, exonerando as entidades que não têm as capacidades financeiras para ver o seu tráfego a ser tratado da mesma forma. Por fim, os utilizadores têm muito a perder com a não aplicação de políticas de *net neutrality*, nomeadamente o

2 Disponível em:
https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx#art35

direito à liberdade de expressão, o direito do acesso à informação e a desigualdade [3] que pode existir em conteúdos que exigem um pagamento adicional [4].

A *net neutrality*, ou a falta dela, é um grande problema debatido no mundo inteiro. Existem motivações válidas tanto para quem está de acordo com a aplicação de políticas de *net neutrality*, como para quem está contra. Um regime híbrido capaz de mitigar os problemas de ambas as partes seria o ideal, no entanto, a importância deste tema sobressai quando se questionam direitos fundamentais em troca de valores, sobretudo, económicos. Segundo Barry Diller, fundador da *Fox Broadcasting Company*, as oportunidades que a *internet* trouxe, não devem ser alteradas [5].

De forma a abordar os problemas da *net neutrality*, as legislações inerentes à mesma e as nuances mais relevantes deste tema, o presente trabalho ficou arquitetado da seguinte maneira:

Inicialmente, será explicado com algum detalhe o porquê de surgirem problemas em órbita da *net neutrality*, que problemas são esses, e porque as partes contra e a favor da *net neutrality* devem ser ambas ouvidas. De seguida, as abordagens adotadas pela América ao longo dos últimos anos para lidar com este assunto serão analisadas em conjunto com alguns tópicos presentes na mais recente legislação. Por último, será analisada a abordagem europeia no mesmo enquadramento que a americana. De referir que ao longo do documento serão estudados problemáticas gerais da *net neutrality* que se considerem relevantes.

3 O Princípio da igualdade deve ser assegurado na condição de haver serviços que exigem mais de um ponto de vista financeiro. "O princípio da igualdade impõe aos poderes públicos um tratamento igual de todos os seres humanos perante a lei e uma proibição de discriminações infundadas, sem prejuízo de impor diferenciações de tratamento entre pessoas, quando existam especificidades relevantes que careçam de proteção", disponível em: https://dre.pt/web/guest/lexionario/-/dj/117357316/view

4 O jornalista *Thor Benson*, expõem de forma clara que a liberdade de expressão deve ser disseminada de igual forma por todos, caso contrário, o uso desta torna-se assimétrico. "*There is no free expression when you have to pay extra to stand on the soap box*".

5 Barry Diller dita, e bem, que a *internet* permite a qualquer um publicar o seu próprio conteúdo sem qualquer censura. "*The Internet came together as a miracle, really. Anyone with a wire can publish, we need to keep it that way*".

2. *Not Neutrality*

A ideia de que o mundo estaria envolvido em redes de partilha de informação, é uma ideia bastante antiga edificada por *Nikola Tesla* no início de 1900. Mais tarde, no início de 1960, *J. C. R. Licklider* introduziu a ideia de uma "rede intergaláctica" que interconectava vários computadores e que permitia a troca de informação através de porções de dados, designados de pacotes. A criação desta ideia, inicialmente para fins militares e científicos, funde-se no princípio da existência de uma rede universal que dá o poder aos seus utilizadores de se expressarem livremente e de acederem de forma ilimitada à informação [6].

A Internet abriu um novo mundo de oportunidades para o ser humano e deve ser vista como o produto da inovação e da criatividade do ser humano. Por ser um produto da sua autoria tem o propósito de aprimorar as suas necessidades e, neste momento, é indubitavelmente uma das mais importantes ferramentas de comunicação. Pelas suas características, permite o acesso quase ilimitado a infinitas fontes de informação distintas e de uma forma discutivelmente rudimentar.

A dependência das tecnologias, em particular da *internet*, acabou por levantar questões, que nada têm a ver com a tecnologia, sobretudo questões económicas e de interesse estratégico. Um dos debates mais acesos segundo a *Microsoft*, é a questão da *net neutrality*[7]. Este paradigma dita que todos os *bits* devem ser tratados de forma igual, desde o momento que são transmitidos até ao fim da sua viagem, instituindo, portanto, que os responsáveis pelo transporte não os possam manipular. Isto implica que o tráfego não seja bloqueado, discriminado nem retardado por qualquer que seja o motivo. A *not neutrality* (não existência de *net neutrality*) é análogo a dar o poder aos ISP para que tratem a informação da forma que assim desejarem, incluindo o favorecimento dos seus próprios interesses. Caso não se debata sobre a *net neutrality*, não só os ISP terão as

6 Disponível em: https://www.history.com/news/who-invented-the-internet
7 Em 2018 a *Microsoft* lançou um relatório acerca dos 10 maiores problemas que a tecnologia enfrenta, o problema da *net neutrality* surge em 8ª posição demonstrando a sua relevância. Disponível em: https://blogs.microsoft.com/wp-content/uploads/2018/01/TopTen2018.pdf

habilidades técnicas para pôr em prática uma política de *not neutrality*, como jurídicas.

Todavia a neutralidade da rede tem significados diferentes para várias pessoas. Alguns querem tratamento igual para todos os bits, outros querem apenas tratamento igual para todos os ISP, outros afirmam que as operadoras deveriam poder cobrar mais por serviços premium, mas não bloquear ou restringir o acesso a conteúdos. Cada abordagem tem implicações diferentes para o gerenciamento de rede e consequências diferentes para as partes envolvidas.

A verdade é que a *net neutrality* tem permitido que qualquer entidade possa ter uma iniciativa livre, sem restrições à sua prosperidade. Apenas se consegue uma iniciativa livre obedecendo ao princípio da liberdade de expressão [8], as entidades e os serviços que hoje associamos inconscientemente como sendo a "internet", apenas coexistem porque lhes foi concebido o espaço para sonhar e desenvolver [9] e se assim não fosse, a evolução da *internet* não teria existido devido à falta de escolha, competição, inovação e oportunidades.

É exatamente o problema da *not neutrality* que tem gerado discordância entre os ISP, os fornecedores de serviço e os utilizadores finais. Por um lado, os ISP e os criadores de serviço pretendem oferecer um serviço com mais qualidade aos seus clientes, para isso, exigem a liberdade de gerir os serviços da forma que eles entenderem. Por outro lado, as entidades que não têm recursos financeiros para equiparar as práticas exercidas pelas empresas mais poderosas são automaticamente impossibilitadas de criar o seu espaço de negócio de forma justa. Por último, os consumidores tipicamente preferem aceder a serviços e conteúdos sem tratamento diferenciado, como pode ser verificado no estudo perpetrado pelo *Body of European Regulators for Electronic Communications* (BEREC) em 2015

8 O Ponto 1 do artigo 37 da Constituição Portuguesa (princípio da liberdade de expressão) protege este princípio ditando que "Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações."

9 A Google transcreve o seguinte: "*Thanks in part to net neutrality, the open internet has grown to become an unrivaled source of choice, competition, innovation, free expression, and opportunity. And it should stay that way*". Novamente, mostrando o papel relevante da *net neutrality* no crescimento da *internet*. Disponível em: https://www.google.com/takeaction/action/net-neutrality

[10], que visa perceber qual é a posição dos utilizadores mediante o valor da *net neutrality*.

Nunca na sua criação a *internet* teve um intuito comercial. Em paralelo, a área das comunicações *broadband* demonstrava que o valor económico era efetivamente um fator que se destacava. No contexto das telecomunicações o operador nunca teve o direito de escolher com quem as pessoas podiam falar, nem o direito de editar o conteúdo das suas conversas, não existindo, portanto, uma manipulação dos conteúdos que fluíam por estas redes de comunicação nem a aplicação de políticas de *not neutrality* visíveis.

Durante a última década, foi visível a transição de utilizadores que maioritariamente acediam a informação por meios que não a *internet*, quer seja com o *pack* de canais ou mesmo com o telefone de casa, para um utilizador que efetua chamadas através da *internet* (via *WhatsApp*, *Messenger*, entre outras) e, igualmente, vê o seu conteúdo televisivo através da *internet* (via *Netflix*, *HBO*, *Amazon Prime*, entre outras). Não só existe um impulso natural para as novas gerações gostarem da liberdade e riqueza que a *internet* tem a oferecer comparativamente aos meios tradicionais, como exige menos esforços económicos para o efeito. Notoriamente, a receita dos prestadores de serviço (ou a falta dela) não é a idealizada, dada a força natural desta transição. É claro que estas entidades subsistem dos serviços prestados aos clientes e por isso, este é um fator relevante a ter em conta, evidentemente que a falta de investimento nos ISP é um problema, no entanto, uma política de *not neutrality* pode acabar com vários direitos básicos dos utilizadores, bem como uma competitividade construtiva dos prestadores destes serviços.

Uma das metodologias que os ISP podem adotar para combater este problema é olhar para os serviços que geram mais tráfego pelo utilizador e, tendo em conta que o fornecem e não têm benefícios acrescidos com isso, podem tornar este paradigma num modelo de negócio cobrando mais aos utilizadores para que

10 Disponível em: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5024-berec-report-on-how-consumers-value-net-neutrality-in-an-evolving-internet-marketplace-a-report-into-ecosystem-dynamics-and-demand-side-forces

esse seja um serviço diferenciado e com melhor acesso do que os restantes, esta prática é muitas vezes designada de "*fast lane*"[11]. Evidentemente o criador desse serviço também estará interessado em que o seu serviço seja entregue com a melhor qualidade possível e pode também demonstrar o seu interesse estabelecendo acordos com o prestador de serviço para garantir a qualidade de entrega do seu serviço.

Existem países mais reservados que claramente não concordam nem aplicam políticas de *net neutrality*, nem o próprio estado nem as suas entidades estão interessados em ter competição produtiva, nem ideias contrárias aos seus próprios princípios. Por um lado, e não sendo de todo errado, a *not neutrality* beneficia o mercado nacional com mais investimentos nos ISP e eventualmente nos fornecedores desse serviço. O problema surge quando os prestadores de serviço têm um controlo total sobre os bits que transmitem e usam esse poder para benefício próprio deixando para trás todos os direitos e oportunidades associadas à *net neutrality* [12].

O ideal nesta colisão de interesses é que nenhum direito dos utilizadores seja comprometido e que nenhuma oportunidade que tenha surgido com a *internet* se desvaneça, assegurando sempre a continuidade da inovação e do conhecimento. Paralelamente, deve-se procurar uma forma de aumentar o investimento nos ISP sem nunca comprometer a competitividade entre estes nem das organizações que usam a *internet* como parte da sua infraestrutura.

2.1. Solução Prática

Na prática, o que acontece com a atual ligação que os ISP prestam aos seus clientes pode ser vista como um cabo dividido em duas partes. Uma das partes é

11 Ideia debatida muito cedo por *Tim Wu*, que se tornou num tema muito debatido dos dias de hoje. Disponível em: https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2282&context=faculty_scholarship

12 Também o Facebook já demonstrou a sua posição sobre a temática da *net neutrality*, transcrevendo o seguinte: "*If we want everyone in the world to have access to all the opportunities that come with the internet, we need to keep the internet free and open*". Disponível em: https://www.facebook.com/zuck/posts/10103878724831141

dedicada aos canais televisivos, nesta divisão existe uma descrição completa do ISP para mostrar os conteúdos que desejarem, podendo até mostrar o seu próprio conteúdo como se acredita que foi feito pela *Verizon* quando aplicou medidas para retardar o tráfego da *Netflix* de forma a anunciar a sua plataforma *Hulu* [13]. Na outra divisão encontra-se a *internet*, em que existe um fluxo bidirecional completamente livre de tratamento e sem qualquer restrição. Uma das soluções dos ISP é enviar um certo conteúdo (como por exemplo, a *Netflix*) que tipicamente usa a via da *internet*, pela via em que os próprios têm descrição. Tecnicamente, isto é possível, ambos usam mecanismos de transmissão idênticos (*IP protocol*) com propriedades elétricas idênticas que permitem a transmissão desses *bits* de uma divisão para a outra.

Usando este paradigma, pode existir algum problema futuro para qualquer uma das partes? Pode. Nada impede a *Netflix* de querer comprar uma *fast lane* e, na prática, este ato, só por si, não é errado, deve existir prioridade de vários serviços, como serviços médicos, chamadas de emergência, comunicações dos alarmes, entre outros. Pondere, no entanto, que todos os fornecedores de serviço (com capacidade monetária), decidem colocar o seu serviço numa *fast lane*, chega uma altura em que a divisão da *internet* passa a ser tão reduzida que será vestigial. Assumindo que os débitos não são alterados por cada vez que é introduzido um serviço na via operada pelo ISP, as capacidades de débito geral não mudam, podendo mesmo chegar ao ponto de o canal da *internet* ficar inoperável.

Como resolver este problema agradando todas as partes? Uma das respostas que aparenta ser óbvia, mas que tem potencialidade é aumentar ambas as divisões das ligações do ISP ao mesmo ritmo, para que nenhuma delas possa ser mais beneficiada. Claramente isto traz outros problemas inerentes, o débito praticável tem limitações conhecidas, principalmente quando se fala de ligações *wireless*. No entanto, isto não deve ser encarado como um problema, mas sim como uma oportunidade de evolução, é precisamente quando surgem problemas deste cariz

13 Disponível em: https://www.digitaltrends.com/web/verizon-wireless-throttling-video-traffic/

que existe espaço para a inovação [14]. O que não deve acontecer é permitir que a divisão da *internet* passe a meros vestígios por motivos, sobretudo, económicos.

14 Opinião do *Massachusetts Institute of Technology* (MIT) *Media Labs*. Disponível em: https://www.youtube.com/watch?v=AdANAZ-bk44

3. Abordagem Americana

Dada a sua relevância, a *net neutrality* é um tema discutido mundialmente, no entanto, o debate sobre a *net neutrality* nos EUA fez eco, primeiro, porque começou bastante cedo, segundo, porque o debate foi rico o suficiente para outros estados subscreverem ideias resultantes do debate. Em 2010, a *Federal Communications Commission* (FCC) vigorou um conjunto de regras capazes de controlar a *net neutrality* e reforçar a importância da liberdade de expressão, inovação, aumento do investimento, competição, criação de emprego e crescimento económico [15].

Em 2015, surgiu um novo conjunto de regras muito bem encarado pela maioria da população americana, que trouxe várias nuances importantes para a regulação do acesso à *internet*[16]. Este regulamento introduziu 3 princípios fundamentais para o cumprimento de uma política de *net neutrality*, dos quais, o *no blocking*, que proíbe o bloqueio de serviços, aplicações e tráfego; o *no throttling*, que proíbe a redução ou o aumento da velocidade de *download* ou *upload* de um dado conteúdo; e o *no paid prioritization*, que proíbe o benefício de certos conteúdos em troca de um investimento adicional, três princípios aplicados assumindo que se trata de conteúdo lícito.

A correta implementação de uma política de *no paid prioritization* proposta pela FCC, anula as *fast lanes* referidas no capítulo 2. No entanto, repare-se que esta limitação pode, e é ultrapassada com o uso de *Content Delivery Networks* (CDNs) que permitem a entrega de conteúdo com menos latência, providenciando um acrescido aumento de qualidade do serviço em troca de dinheiro. Segundo um estudo feito pela empresa alemã *Statista*, estima-se que em 2022 o uso de CDN

15 Disponível em: https://docs.fcc.gov/public/attachments/FCC-10-201A1_Rcd.pdf. "*Today the Commission takes an important step to preserve the Internet as an open platform for innovation, investment, job creation, economic growth, competition, and free expression*".
16 Disponíveis em: https://www.fcc.gov/document/fcc-releases-open-internet-order

aumente cerca de duas vezes comparativamente com o ano atual (2020)[17], demonstrando o real interesse por esta tecnologia.

O uso desta tecnologia é bastante adotado, principalmente pelos serviços *Over the Top* (OTT), serviços livremente acessíveis pela *internet* que, usualmente, são os mais consumidos pelos utilizadores, são exemplos o *WhatsApp*, o *Spotify*, o *Google*, o *Skype*, entre muitos outros. Segundo um estudo de 2017 efetuado pela ANACOM[18], 44% dos utilizadores portugueses fizeram chamadas de vídeo ou voz pela Internet, podendo-se aferir, que existe uma tendência para o uso dos serviços OTT que são, tipicamente, disponibilizados através da *internet*. Com base nesta transição de serviços, os ISP adaptam as suas ofertas disponibilizando uma maior quantidade de dados móveis, oferecendo serviços OTT nos seus pacotes ou mesmo criando e disponibilizando os seus próprios serviços. Na prática, os OTT acabam por ser o grande potencial de desequilíbrio quando se fala de neutralidade de rede pois são os que têm mais capacidade de investimento, é precisamente neste termo que a regulação é imprescindível.

No dia 11 de junho de 2018 a FCC introduziu um novo pacote regulamentar [19] que vem alterar grande parte dos princípios de acesso à *internet* introduzidos pelo antigo regulamento "*Open Internet Order*", permitindo que os operadores de serviço manipulem o tráfego de forma muito mais soberana, autorizando, inclusive, a implementação de políticas de *paid prioritization* e *throttling*, medidas opostas às previamente propostas. Essencialmente, teme-se que as operadoras usam este poder para priorizar tráfego em prol do seu próprio benefício, podendo até dar primazia aos seus próprios produtos. Nesta condição os ISP deixam de ser exclusivamente transportadores de serviço para serem criadores de serviço, o que lhes permite a liberdade de expressão e a proteção dada pelo "*first amendment"* da constituição americana [20].

Para além dos seus próprios produtos, com este novo regulamento, o operador tem margem estratégica para acordar com organizações, tipicamente

17 Disponível em: https://www.statista.com/statistics/267184/content-delivery-network-internet-traffic-worldwide/
18 Disponível em: https://www.anacom.pt/render.jsp?contentId=1404697
19 Disponível em: https://www.fcc.gov/restoring-internet-freedom
20 Disponível em: https://constitution.congress.gov/constitution/amendment-1/

serviços *OTT*, e ajudarem-se mutuamente através de investimentos para um melhor tratamento do seu tráfego. Infelizmente, estes acordos não são inéditos e já aconteceram no passado [21]. A título exemplificativo, a *AT&T* bloqueou o tráfego *VoIP* do *Skype* de forma a reduzir o holofote que era colocado sobre o seu competidor, também a Verizon bloqueou a *Google Wallet* para favorecer o seu *software* de pagamentos de serviços [22].

Numa entrevista dada ao *The Daily Signal* pelo presidente da FCC[23], Ajit Pai, o mesmo refere que desde o regulamento de 2015 que deixou de haver tanto investimento nas operadoras e que os ISP têm medo de inovar com base nas legislações impostas por essa versão do regulamento. Este é o grande motivo que justifica as novas medidas impostas pela regulação de 2018. Em relação à liberdade que permite aos operadores a divisão do tráfego para a via que têm total controlo, segundo a FCC, este não é tema que mereça preocupação porque as operadoras têm de ser transparentes em relação às medidas de tráfego que querem implementar e as mesmas serão escrutinadas pela FCC. Adicionalmente, a FCC acredita que esta questão não se trata das regulações impostas pelo novo pacote regulamentar, mas sim, de uma questão competitiva, dado que a transparência dos operadores em relação à temática da neutralidade de rede aumenta a competição na medida em que os clientes não satisfeitos podem sempre alterar o seu serviço.

Em relação aos benefícios evidenciados que os operadores e fornecedores de serviço passam a ter com este novo regulamento, é dito que o problema da *net neutrality* não é o bloqueio de conteúdos lícitos perante os utilizadores, é sim, o desejo destes terem acesso rápido e barato à *internet*. Em resposta a este problema, o novo regulamento dá mais liberdade de ações aos ISP para que estes construam redes de maior qualidade e facilidade de acesso, o que aparenta ser incoerente devido ao incremento dos preços praticados por estes.

A verdade é que este novo regulamento pode degradar o serviço de organizações que não sejam parceiras dos ISP, bem como as organizações que não

21 4 casos práticos passados desta prática estão disponíveis em: https://www.theverge.com/2018/6/11/17438638/net-neutrality-violation-history-restoring-internet-freedom-order
22 Disponível em: https://www.businessinsider.com/verizon-blocking-google-wallet-201
23 Disponível em: https://www.youtube.com/watch?v=8uR2rxfJtFY

sejam capazes de competir com os "*big players"*. Na teoria, a competição entre operadoras impede que este desfavorecimento aconteça, permitindo um maior leque de escolha. Na prática, a competição entre operadoras acaba por não ser uma realidade tão presente ao ponto de permitir esta escolha [24], possibilitando que as operadoras sejam livres para restringir o acesso a certos conteúdos e que cobrem mais pelos serviços que entenderem.

O desagrado geral pela nova ação da FCC, que foi considerada arbitrária, inconstante e em violação perante a Lei do Procedimento Administrativo (que rege o processo pelo qual as agências federais desenvolvem e emitem regulamentos), fez-se notar, seja por meio de legislações estaduais ou através de contestações em tribunais federais. Certos estados aprovaram uma legislação que reflete as regras de neutralidade da rede propostas por Wheeler no regulamento "*Open Internet Order*", precisamente por não subscreverem as ideias deste novo regulamento. Para consultar com mais rigor as ações tomadas por certos estados no âmbito da nova legislação inerente à *net neutrality* pode ser consultado o artigo da *National Conference of State Legislatures* (NCSL) [25]. Como prova de insatisfação ao novo regulamento, a comissária Jéssica Rosenworcel escreveu um documento em que expõe a sua opinião sobre o mesmo iniciando com a frase arrebatadora "*net neutrality is internet freedom*", opinando que este regulamento está a retirar a liberdade que a *internet* trouxe[26].

A discussão política sobre a adoção de medidas de *net neutrality* muitas vezes deixa para trás o aspecto técnico da implementação de sistemas que garantem neutralidade de rede. A perceção de que os estudos técnicos destas abordagens ficam em segundo plano é bastante presente, no entanto, pouco falada. Onde são contempladas as políticas de *Quality of Service* (QoS)? Fazendo uma analogia ao tráfego de circulação, existem vias distintas para tráfego distinto, a circulação nas autoestradas carece de veículos com uma requisição específica, da mesma forma que existem vias de emergência para as ambulâncias ou mesmo as ecopistas para os peões e bicicletas. O mesmo se aplica ao tráfego de rede, existem

24 Tema debatido com mais rigor em: https://www.theverge.com/2018/6/11/17439456/net-neutrality-dead-ajit-pai-fcc-internet
25 Disponível em: https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2020-legislation.aspx
26 Documento disponível em: https://docs.fcc.gov/public/attachments/FCC-17-166A6.pdf

aplicações com requisições diferentes, por exemplo, uma chamada de telefone via *internet* (VoIP) tem prioridades que um *download* de uma aplicação não tem.

Tratar todos os bits de forma igual para efeitos de gestão de tráfego tem sentido literal, é análogo a não aplicar nenhum tratamento na transmissão de informação. Se esta política fosse seguida, é correto dizer que a evolução das comunicações que são hoje efetuadas estariam muito aquém das praticadas atualmente. Trata-se de uma política bastante fácil de aplicar na prática e é defendida por entidades como a "grande" *Electronic Frontier Foundation* (EFF). Adicionalmente, Jeremy Gillula, membro da EFF, afirma que o tráfego cifrado não pode ser examinado de forma a aferir a necessidade da política de prioridade de tráfego [27]. De salientar que as medidas de gestão de tráfego excepcionais apenas são aceites se forem comprovadamente baseadas em critérios técnicos, isto é, para efeitos de QoS, os operadores têm de demonstrar tecnicamente a dependência destas medidas para o correto funcionamento da rede.

A abordagem americana acaba por ser muito rica na quantidade de valências que tenta resolver. É notória a satisfação e sucesso dos fornecedores de serviço, ainda é mais notário o sucesso dos criadores de serviço americanos uma vez que são, indiscutivelmente, os maiores do mundo e os mais avançados tecnologicamente. Teme-se, no entanto, que com a nova regulação imposta pela FCC os fornecedores de serviço retirem as oportunidades intrínsecas a uma boa política de *net neutrality*, bem como os direitos dos seus utilizadores.

27 "*network operators shouldn't be doing any sort of discrimination when it comes to managing their networks*". Disponível em: https://spectrum.ieee.org/telecom/internet/net-neutralitys-technical-troubles

4. Abordagem Europeia

Apesar da *not neutrality* passar despercebida, pela relevância que tem no contexto europeu, a União Europeia (EU) introduziu um pacote regulamentar que disciplina de forma concisa o acesso à *internet* e a manipulação do seu tráfego. A abordagem europeia é encontrada no Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 [28]. Este regulamento também altera a Diretiva 2002/22/CE [29] relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, bem como o Regulamento (UE) nº 531/2012 [30] relativo à itinerância nas redes de comunicações móveis públicas da União. O objetivo do regulamento 2015/2120, aprovado em agosto de 2016, pode ser encontrado logo no 1º ponto do 1º artigo com a seguinte constatação "*O presente regulamento estabelece regras comuns para garantir o tratamento equitativo e não discriminatório do tráfego na prestação de serviços de acesso à Internet, e os direitos conexos dos utilizadores finais*". Nesta frase sobressai a clara preocupação por um acesso à *internet* de forma neutra, sem discriminação e justa. Este regulamento é aplicável a todos os prestadores de serviço de acesso à *internet* [31] e assenta em 4 conjuntos de regras fundamentais para a temática da *net neutrality*.

Em **primeiro**, o ponto 1 do artigo 3º (Garantia de acesso à Internet aberta), que dita que "*Os utilizadores finais têm o direito de aceder a informações e conteúdos e de os distribuir, de utilizar e fornecer aplicações e serviços e utilizar equipamento terminal à sua escolha, através do seu serviço de acesso à Internet, independentemente da localização do utilizador final ou do fornecedor, ou da localização, origem ou destino da informação, do conteúdo, da aplicação ou do*

28 Dado que se trata de um regulamento e não carecendo de transposição, o mesmo passa a ter efeito direto sobre a legislação portuguesa. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015R2120&from=PT

29 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0022&from=PT

30 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012R0531&from=EN

31 Este regulamento remete para o BEREC, organismo que agrupa os Reguladores de Telecomunicações europeus. Posteriormente, o BEREC remete algumas linhas de orientação para a implementação do regulamento pelos reguladores nacionais, no caso de Portugal, a ANACOM. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015R2120

serviço", demonstrando uma clara relação à política de *non blocking* estabelecida pela FCC, efetivando a liberdade do utilizador em aceder e distribuir o conteúdo que desejar, independentemente dos fatores envolventes. Desta forma é assegurado o princípio da liberdade de expressão[32] que consta na Constituição portuguesa, não existindo censura de conteúdos (exceto os ilícitos).

Em **segundo,** o ponto 3 do 3º artigo (Garantia de acesso à Internet aberta), que consegue ser resumido no seu primeiro parágrafo "*Os prestadores de serviços de acesso à Internet tratam equitativamente todo o tráfego, ao prestarem serviços de acesso à Internet, sem discriminações, restrições ou interferências, e independentemente do emissor e do recetor, do conteúdo acedido ou distribuído, das aplicações ou serviços utilizados ou prestados, ou do equipamento terminal utilizado*". Neste parágrafo depreende-se bem a posição do BEREC para que os operadores e as entidades economicamente mais poderosas não sejam as favorecidas no que toca ao tratamento do seu tráfego.

O segundo parágrafo deste artigo nitidamente remete para o QoS [33], apesar deste segundo parágrafo não ser explícito para muitos juristas no que toca à exclusividade da aplicação de medidas razoáveis de gestão do tráfego sobre aspetos técnicos, o texto é esclarecedor em relação à necessidade de justificações técnicas que, como já foi visto, também foram propostas pela FCC e são extremamente necessárias para um bom funcionamento das redes.

O terceiro parágrafo remete para a política de *no throttling* [34], também implementada pela FCC. Era expectável que o bloqueio, abrandamento, alteração,

32 Ponto 2 do artigo 37 da Constituição Portuguesa (princípio da liberdade de expressão), este dita que "O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura."

33 Artigo 3, ponto 3, 2º paragrafo do regulamento 2015/2120, "O primeiro parágrafo não obsta a que os prestadores de serviços de acesso à Internet apliquem medidas razoáveis de gestão do tráfego. Para que possam ser consideradas razoáveis, essas medidas devem ser transparentes, não discriminatórias e proporcionadas, e não podem basear-se em questões de ordem comercial, mas sim na qualidade técnica objetivamente diferente dos requisitos de serviço de categorias específicas de tráfego. Essas medidas não podem ter por objeto o controlo de conteúdos específicos, nem podem ser mantidas por mais tempo do que o necessário."

34 Artigo 3, ponto 3, 3º paragrafo do regulamento 2015/2120, "Os prestadores de serviços de acesso à Internet não podem estabelecer medidas de gestão do tráfego mais gravosas do que as medidas previstas no segundo parágrafo, e, em particular, não podem bloquear, abrandar, alterar, restringir, ou degradar conteúdos, aplicações ou serviços específicos, ou categorias específicas dos mesmos, nem estabelecer discriminações entre eles ou neles interferir, exceto na medida do necessário ..."

restringimento ou a degradação dos conteúdos fossem medidas devidamente proibidas, exceto se usadas em situações muito próprias, descritas nas alíneas a), b) e c).

A **terceira** nuance que este regulamento introduz de alto relevo pode ser encontrada no 1º ponto do 4º artigo (Medidas de transparência para garantir o acesso à Internet aberta). A existência deste artigo assegura que os prestadores de serviço sejam transparentes e objetivos no contrato estabelecido com o cliente, em particular nas medidas de gestão de tráfego e o impacto que elas possam ter para o uso da *internet* pelo utilizador[35]. À semelhança do que acontece com o já descrito no capítulo 3, a existência de transparência por parte dos operadores de serviço permite uma maior competição na medida em que o utilizador escolhe o serviço que deseja com base na sua satisfação.

Por último, a **quarta** nuance pode ser encontrada no 5º ponto do 3º artigo (Garantia de acesso à Internet aberta), onde são mencionadas as especificações para a implementação e uso dos serviços *Premium.* Estes serviços são facilmente associados como sendo discordantes à regra do *no paid prioritization* criada pela FCC que visa proibir o benefício de certos conteúdos em troca de um investimento adicional. Em adição a esta prática de desfavorecimento pelas entidades que não suportam pagar esta *fast lane,* existe o facto de que os fornecedores de serviço podem usar CDN, como já referido, incrementando ainda mais a qualidade de disseminação do seu conteúdo em troca de dinheiro.

A liberdade que os prestadores e os fornecedores de serviço têm para oferecer serviços diferenciados relativamente aos serviços de acesso à *internet* é descrita no primeiro parágrafo do 5º ponto do 3º artigo [36], concluindo que pode existir a entrega e o uso de serviços *Premium* para determinados fins, como por

35 Artigo 4, ponto 1, alínea a) "Informações sobre o impacto que as medidas de gestão do tráfego aplicadas pelo prestador de serviços poderão ter na qualidade do serviço de acesso à Internet, na privacidade do utilizador final e na proteção dos seus dados pessoais "

36 Artigo 3, ponto 5, 1º paragrafo do regulamento 2015/2120, "Os prestadores de serviços de comunicações eletrónicas ao público, incluindo os prestadores de serviços de acesso à Internet, e os fornecedores de conteúdos, aplicações ou serviços têm a liberdade de oferecer serviços diferentes dos serviços de acesso à Internet que estejam otimizados para conteúdos, aplicações ou serviços específicos, ou para uma combinação dos mesmos, caso a otimização seja necessária para respeitar os requisitos dos conteúdos, aplicações ou serviços para um nível de qualidade específico."

exemplo, serviços IPTV, *VoLTE*, serviços corporativos, entre outros. Isto significa que modificar a qualidade e a disponibilidade de um serviço de uma perspetiva técnica e legal é possível.

A solução dada no capítulo 2 relativamente ao perigo do canal da *internet* se tornar meros vestígios com a introdução de vários serviços no canal controlado pelo ISP acaba por ser referida no segundo parágrafo do 5º ponto do 3º artigo "Esses serviços não podem poder ser utilizados nem oferecidos em substituição dos serviços de acesso à Internet, nem podem afetar a disponibilidade ou a qualidade geral dos serviços de acesso à Internet para os utilizadores finais", existindo uma salvaguarda à capacidade da rede para oferecer ou facilitar serviços controlados pelo ISP e garantindo em simultâneo que o canal da *internet* não se torna inexistente.

Referir por último que este regulamento não refere sobre práticas *zero rating*, sendo por isso bastante criticado. O *zero rating* é a prática de fornecer acesso à *internet* sem custos financeiros sob certas condições, tipicamente manifesta-se no fornecimento de serviços incluídos num pacote em que esses serviços não são contabilizados. Esta prática pode implicar impactos negativos para a concorrência, na medida em que os seus serviços têm custos acrescidos comparativamente aos que estão cobertos por uma política de *zero rating*. Este é um exemplo de *not neutrality* e um manifesto do poder que os ISP têm para praticar a *not neutrality*. Na opinião de Senador Ro Khanna, os serviços que pratiquem políticas de *zero rating*, como a MEO, começam a dividir a própria *internet* em pacotes[37]. Na prática, estas políticas estão a bloquear certos serviços a não ser que sejam explicitamente pagos.

Também o 5º ponto do 3º artigo 3 foca a necessidade do acesso não discriminatório à *internet*, motivando as autoridades a aplicarem as medidas necessárias para o correto e justo funcionamento das redes. A autoridade (ANACOM), deve verificar e garantir que as políticas de gestão de tráfego são bem aplicadas, monitorizar esta atividade para assegurar que os utilizadores finais não são lesados e aplicar as devidas sanções. O 6º artigo, referente às sanções, dita

37 *Tweet* disponível em: https://twitter.com/RoKhanna/status/923701871092441088

que os estados-membros devem estabelecer o regime de sanções e comunicá-lo à comissão até 30 de abril de 2016 [38]. No dia 04 de abril de 2020 com o Decreto-Lei n.º 49/2020[39] é estabelecido o regime sancionatório aplicável à violação de regras sobre acesso à *internet* aberta, fazendo com que este regime passe a estar incluído na Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro), no capítulo "supervisão e fiscalização", passando a constar do regime das sanções aplicável à violação de obrigações previstas no Regulamento n.º 2015/2120 e no Regulamento n.º 531/2012**.**

Com algum tempo de atraso este decreto-lei veio clarificar como serão perpetuadas as coimas para as contraordenações na temática da *net neutrality*, ou da falta dela. São tipificadas as contraordenações graves, punidas com coimas cujo montante varia entre 250,00 e 1.000.000,00 euros, a violação das obrigações enumeradas nos n.ºs 4 e 6, do artigo 113.º, da Lei das Comunicações Eletrónicas. Também é tipificada a contraordenação muito grave, punida com coimas cujo montante varia entre 750,00 e 5.000.000,00 euros, da violação das obrigações enumeradas nos n.ºs 5 e 7, do artigo 113.º da Lei das Comunicações Eletrónicas [40]. Estas contraordenações acabam por abranger uma panóplia de violações puníveis, das quais o não uso de políticas de *net neutrality* faz parte.

Para concluir, no dia 30 de abril de 2019, o regulamento 2015/2120 foi sujeito a uma reavaliação pelo Parlamento Europeu e do Conselho sobre as medidas propostas [41]. A conclusão desta reavaliação foi a seguinte: "*Compared with the situation in 2015, before the regulation applied, end-users and content application providers express great satisfaction with today's state of affairs. Internet service providers also support the principles of an open internet and do not consider that it is necessary to amend these principles*" culminando em

38 Artigo 6 do regulamento 2015/2120, "Os Estados-Membros estabelecem o regime de sanções aplicável às infrações ao disposto nos artigos 3.o, 4.o e 5.o e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Os Estados-Membros notificam essas disposições à Comissão até 30 de abril de 2016, e notificam-na sem demora de quaisquer alterações subsequentes das mesmas"
39 Disponível em: https://dre.pt/web/guest/home/-/dre/139472786/details/maximized?serie=I&print_preview=print-preview
40 Disponível em: https://www.servulo.com/pt/investigacao-e-conhecimento/Violacao-de-regras-sobre-acesso-internet-aberta-e-chamadas-intra-Uniao-Europeia-reguladas-um-regime/7193/
41 Relatório disponível em: https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-203-F1-EN-MAIN-PART-1.PDF

satisfação tanto dos utilizadores como dos prestadores e fornecedores de serviço. Como consequência, a comissão constata que não é apropriado propor emendas ao regulamento nesta fase demonstrando o efeito positivo do mesmo, verdade seja dita, a forma como o regulamento joga com os interesses das partes envolvidas do debate sobre a neutralidade de rede torna espectável a satisfação geral das partes.

5. Considerações Finais

Pelo seu perigo inerente, a *net neutrality* é um tema merecedor de debate e de consideração por parte dos estados e das entidades reguladoras. Neste documento procurou-se abordar os problemas subjacentes às políticas de *not neutrality*, o porquê de existirem esses problemas e quais são as soluções propostas pelas legislações Americana e Europeia para combater esta ameaça.

Contrariamente ao que se pensa, foi possível verificar que a aplicação de políticas de *Quality of Service* (QoS) não é sinonimo de *not neutrality*, pelo contrário, a aplicação destas políticas é extremamente importante para que a *internet* tenha a maior eficiência possível. É necessário estar ciente da existência de várias definições para o conceito de *net neutrality*. Assumindo a definição estrita de *net neutrality*, ou seja, o tratamento igual para todos os bits, nunca houve neutralidade de rede e provavelmente nunca haverá. Uma política de *net neutrality* não deve ser aplicada sobre todos os bits que percorrem a rede, mas sim, deve ser aplicada com o fundamento de que no fim da sua aplicação consegue preservar as oportunidades inerentes à *internet* aumentando em paralelo a *performance* da mesma.

No debate da *not neutrality*, não são apenas os utilizadores que têm um risco associado, os ISP e os criadores de serviço defendem o seu ponto de vista de uma forma fundamentada, e como tal, também deve ser ouvida. Os ISP desempenham um papel basilar na disseminação do acesso à rede, não só aos utilizadores, como às próprias organizações, hospitais, etc. Apesar dos utilizadores e os ISP cooperarem em prol de um interesse mútuo, em que o utilizador beneficia do acesso à *internet* e o ISP beneficia de uma remuneração, no debate da *net neutrality* existe uma colisão entre ambos que leva à necessidade de que os interesses de ambas as partes sejam salvaguardadas através de um pacote regulamentar.

A abordagem americana sobre a neutralidade da rede acabou por ser muito rica na quantidade de valências que tentou resolver. O regulamento que vigorou

na administração Obama foi muito bem abraçado pelos utilizadores americanos e acredita-se que teve muita influência para o atual regulamento europeu. Com a introdução do novo regulamento americano, liderado pelo presidente da FCC, Ajit Pai, é notória a satisfação dos fornecedores de serviço e dos criadores de serviço americanos pela liberdade legal que têm agora para aplicar medidas de gestão de tráfego que lhes permite beneficiar de uma forma que a anterior regulação não permitia. Teme-se, no entanto, que esta liberdade retire todas as oportunidades que acompanham o verdadeiro motivo da criação da *internet* e que os próprios direitos dos utilizadores passem a estar em causa por motivos, sobretudo, financeiros.

Com a introdução do novo regulamento Americano (*Restoring Internet Freedom*), que tem sido alvo de discussões e revolta, é expectável que parte da liberdade introduzida com este regulamento seja retirada ou retardada na próxima administração. Acredita-se que este regulamento seja exageradamente flexível ao ponto de entregar demasiado poder legal aos ISP para tomarem as decisões que entenderem em prol do seu benefício. Estas decisões podem comprometer direitos fundamentais dos utilizadores e, contrariamente ao que Ajit Pai alega, torna menor a competitividade entre fornecedores e criadores de serviço não cedendo oportunidade aos que têm menos poder financeiro para se estabelecer.

O debate sobre a neutralidade de rede na Europa assume os mesmos problemas e as mesmas questões que proporcionou a criação da legislação americana, no entanto, ao contrário da atual legislação americana acredita-se que a legislação europeia conseguiu um regime híbrido muito bem conseguido.

O regulamento europeu sobre a neutralidade de rede coloca a União Europeia numa posição bastante favorável, privilegiando e dando liberdade aos fornecedores de serviço para que sejam alvo de investimento e fomentando uma maior competitividade entre os mesmos. Em paralelo, permite que os criadores de serviço tenham alguma margem para tornar os seus serviços diferenciados da concorrência, o que é visto por muitos como uma prática errada. Assegurando que o conteúdo *Premium* seja acessível por todos os utilizadores, mas com uma menor qualidade para aqueles que não usufruem verdadeiramente desse serviço, a neutralidade da rede perdura.

Também com este regulamento os direitos dos utilizadores saem reforçados com políticas que garantem que o acesso à *internet* não é indevidamente manipulado. Os problemas associados à *not neutrality*, como o compromisso da inovação e do desenvolvimento não necessitam de uma preocupação gravosa, dado que estas propriedades são asseguradas pelo regulamento e não podem ser colocadas em risco.

Como referido ao longo do documento, existem várias parcelas do regulamento europeu que são em muito semelhantes às primeiras abordagens americanas. Notoriamente, as versões primordiais do regulamento americano focaram essencialmente sobre os direitos dos utilizadores e, nessa vertente, podia-se considerar o regulamento europeu mais flexível, dando alguma liberdade para os ISP gerirem o seu tráfego de forma mais livre, mas nunca colocando em risco os direitos dos utilizadores. Desta forma, a União Europeia encontra-se bem posicionada com a sua regulação sobre a neutralidade da rede, acabando por fomentar a inovação e agradando tanto os consumidores com a liberdade que desejam, como os prestadores e os criadores de serviço com um aumento de investimento e de competitividade.

É necessário mencionar que apesar da reavaliação da União Europeia ditar que o regulamento europeu é bastante híbrido na medida em que agrada todas as partes e completo no seu nível descritivo, tem vários problemas. Sem dúvida que o ponto mais crítico e debatido deste regulamento foi ter deixado de fora a prática de políticas *zero rating* que quando aplicadas colocam em jogo o direito de acesso à informação em troca de pacotes pagos que permitem a um ISP beneficiar, quer através de protocolos com criadores de serviço, quer com o patrocínio do seu próprio serviço. Para além desta prática, o regulamento contém regras que são bastante subjetivas à interpretação e aplicação podendo-se revelar, em certas ocasiões, uma pequena abertura para o uso de políticas de *not neutrality*.

Por último, referir que o maior benefício do regulamento europeu, é precisamente o facto de ser um regulamento e, portanto, diretamente aplicável a todos os estados-membros, não permitindo às legislações nacionais o poder para comprometer os direitos básicos dos utilizadores em prol do benefício económico dos ISP, ou o contrário, o compromisso dos investimentos dos ISP por completo.

Portugal não aparenta ter um papel muito proativo na aplicação de sanções nem da monitorização do tráfego das operadoras em defesa da neutralidade de rede, uma vez que demorou cerca de 4 anos a mais do que o previsto para estabelecer o regime sancionatório aplicável à violação de regras sobre o acesso à *internet* aberta. Apesar disso, a satisfação dos utilizadores e das operadoras portuguesas, aliás, europeias, aparenta ser recíproca.

VISÃO HOLÍSTICA NA SEGURANÇA DE INFORMAÇÃO NAS ESTRUTURAS ORGANIZACIONAIS

JOÃO PAULO LAMEGO *

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestrando em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

O presente trabalho visa abordar uma Visão Holística na Segurança de Informação nas Estruturas Organizacionais, onde o holismo na estrutura organizacional tem como principal objetivo cimentar e desenvolver sinergias e compromisso para atuar com um todo e não na forma individual, exortando a ética, moral e honra.

As empresas enfrentam problemáticas onde o seu "Valor" corre os mais variados riscos, se por um lado pela disrupção tecnológica que torna as empresas mais vulneráveis por outro, devido aos trabalhadores com ausência de valores, onde a ética e moral desvanecem numa sociedade que também enfrenta uma dualidade entre o espaço real e o espaço virtual, sendo cada vez mais dependentes da informação via Ciberespaço.

Conscientes do conflito entre os espaços e pela dependência das tecnologias e Internet, a ética e moral afiguram-se como um novo desafio para as organizações.

Palavras-Chave: Holismo; Segurança da Informação; Cibersegurança; ética.

ABSTRACT

The present work aims to approach a Holistic Vision in Information Security in Organizational Structures, where holism in the organizational structure has as main objective to cement and develop synergies and commitment to act as a whole and not in an individual way, exhorting ethics, morals and honor.

Companies face problems where their “Value” runs the most varied risks, on the one hand due to technological disruption that makes companies more vulnerable on the other, due to workers with no values, where ethics and morals fade in a society that also it faces a duality between real space and virtual space, being increasingly dependent on information via Cyberspace.

Aware of the conflict between spaces and the dependence on technologies and the Internet, ethics and morals appear as a new challenge for organizations.

Keywords: Holistic concept; Information security; Cybersecurity; ethic.

1. Enquadramento

Em Portugal e no Mundo vivemos tempos controversos e preocupantes, onde se assiste a um aumento da criminalidade e um número crescente de vítimas em criminalidade cibernética[1]. Presenciamos uma época onde a sociedade caminha de mãos dadas com o crescimento Tecnológico e a Internet, e assistimos a fenómenos de transformação social[2] nos mais diversos campos da atividade humana.

A Era digital[3] e a sua dependência, está a potenciar a transformação numa sociedade de informação[4], onde não se vislumbram limites a curto prazo, sendo um novo paradigma em processo contagiante, simultaneamente perigoso e igualmente alarmante nos mais variados riscos para as Organizações e a Sociedade.

Parece-me que o futuro assinalará muitos desafios na área das Tecnologias de Informação e Comunicação (TIC), ou também, Tecnologias de Informação, Processos e Comunicação (TIPC), como sugere o autor[5].

1 Aumento da criminalidade cibernética, verificado no Relatório Anual de Segurança Interna (RASI) de 2019 em: https://www.portugal.gov.pt/downloadficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDA0sAAAQJ%2bleAUAAAA%3d

2 Na tradução do artigo de Stephen Castles, lê-se «*Um processo (ou conjunto de processos) que incorpora transformações na organização espacial das relações e das transacções sociais — consideradas em termos da sua extensão, da sua intensidade, da sua velocidade e do seu impacto —, gerando fluxos transcontinentais ou inter-regionais e redes de actividade, interacção e o exercício do poder (Held e outros, 1999: 16).*», vide em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0873-65292002000300008

3 Como definição de Era da informação, (também conhecida como era digital ou era tecnológica) é o período que vem após a era industrial, mais especificamente após a década de 1980; embora suas bases tenham começado no princípio do século XX e, particularmente, na década de 1970, com invenções tais como o microprocessador, a rede de computadores, a fibra ótica e o computador pessoal, retirado de: https://pt.wikipedia.org/wiki/Era_da_informa

4 Nas palavras de Castells, 1999, a sociedade de informação representa verdadeiramente uma nova sociedade. «uma sociedade pode dizer-se nova quando houve uma transformação estrutural nas relações de produto, nas relações de poder e nas relações entre pessoas. Estas Transformações, continua, provocam uma modificação igualmente assinalável na espacialidade e na temporalidade sociais e na aparição de uma nova cultura»

5 Rogério Bravo, Tecnólogo, investigador académico, Inspetor Chefe de Polícia Judiciária, colocado na Secção de Investigação de Criminalidade Informática e Tecnológica, «As tecnologias de informação processamento e comunicação (TIPC) têm lógicas, dinâmicas e leis próprias, leis que nos permitem

Na senda de um futuro melhor creio que a aposta deverá centrar-se nas bases académicas, assim como, na formação e informação.

Outra recomendação que me parece essencial é o reforço da vigilância na penumbra onde realmente acontece a transformação social[6].

A ética e moral aparentemente transcendem a esfera de ação e responsabilidade das organizações, contudo, vêem-se confrontadas diariamente com situações, tais como: roubos, invasão da privacidade, invasão da propriedade, usurpação de dados, mentiras compulsivas dos trabalhadores e jogos dissimulados, atitudes estas, que conduzem à falta de compromisso, lealdade e responsabilidade na função desempenhada.

Os casos ocorrerem internamente e/ou externamente e culminam em incidentes que podem ser puníveis ao abrigo da legislação em vigor.

O Mundo Digital e a Cibersegurança adquirem uma importância preponderante face ao novo paradigma social, sendo a Cibersegurança uma resposta para uma Internet mais segura, contudo, é importante haver consciencialização de boas práticas de utilização no ciberespaço e comportamento dentro da organização.

Citando o clássico da estratégia militar, *Sun Tzu*: *«A arte da guerra ensina-nos a confiar não na ausência do inimigo, mas antes na nossa preparação para a sua chegada, a confiar não na possibilidade de ele não atacar, mas antes em termos tornado a nossa posição inexpugnável.»*. A consciencialização cívica e social no uso da internet será fundamental, é a demonstração mais operativa para nos preparamos.

perspetivar (até hoje e desde que a elas aderimos em massa) um avanço tecnológico significativo, sensivelmente, todos os dois anos e meio.»

6 Complemento com o seguinte texto: «[...] estes garotos são diferentes. Eles estudam, trabalham, escrevem e interagem um com o outro de maneiras diferentes das suas quando você era da idade deles. Eles leem blogs em vez de jornais. Provavelmente nem sabem como é um cartão de biblioteca, que dirá terem um. Ele obtém suas músicas online [...] provavelmente enviam uma mensagem instantânea em vez de pegarem o telefone para marcar um encontro. Conectam-se entre si através de uma cultura comum. Os principais aspetos de suas vidas – interações sociais, amizades, atividades cívicas – são mediadas pelas tecnologias digitais. E não conheceram nenhum modo de vida diferente. (GASSER; PALFREY, 2011, p. 12)», vide em: https://monografias.brasilescola.uol.com.br/historia/estado-sociedade-na-era-informacao-relacao-entre-as-transformacoes-sociais-novas-tecnologias.htm

A globalização[7] renasce sucessivamente com a transformação digital, cujo fenômeno produz profundas alterações na forma como a tecnologia é criada, gerida, instrumentada e comercializada, sendo primordial que a boa informação seja a matriz do conhecimento. De facto, a Segurança e Cibersegurança, têm cada vez mais um papel fundamental na nossa sociedade e organizações, onde as Garantias, Liberdades e Direitos não podem ser alienáveis.

O binómio para o equilíbrio privacidade Vs. segurança será um grande desafio, pois caminhamos a passos largos para uma virtualidade, dependentes e impulsionados pelas tecnologias e internet. Somos constantemente estimulados e manipulados para aceitar as condições comprometedoras e talvez um dia irreversíveis. É interessante pensar em formar uma cultura de defesa, privacidade e segurança com medidas eventualmente híbridas digital & analógico[8], de modo, não ficarmos reféns da tecnologia e conetividade cibernética.

7 Complemento com a definição, «*A globalização é um fenômeno moderno que surgiu com a evolução dos novos meios de comunicação, cada vez mais rápidos e mais eficazes. Há, no entanto, aspetos tanto positivos quanto negativos na globalização. No que concerne aos aspectos negativos, há a referir a facilidade com que tudo circula, não havendo grande controle, como se pode facilmente depreender pelos atentados de 11 de Setembro nos Estados Unidos. Outro dos aspectos negativos é a grande instabilidade econômica que se cria no mundo, pois qualquer fenômeno que acontece num determinado país atinge rapidamente outros países, criando-se contágios que, tal como as epidemias, se alastram a todos os pontos do globo como se de um único ponto se tratasse. Os países, cada vez, estão mais dependentes uns dos outros e já não há possibilidade de se isolarem no seu ninho, pois ninguém é imune a estes contágios positivos ou negativos. Como aspetos positivos, temos, sem sombra de dúvida, a facilidade com que as inovações se propagam entre países e continentes e o acesso fácil e rápido à informação e aos bens. Esta globalização serve para os mais fracos se equipararem aos mais fortes, pois tudo se consegue adquirir através desta grande autoestrada informacional do mundo que é a Internet.*» Vide em: https://pt.wikipedia.org/wiki/Globaliza%C3%A7%C3%A3o,

8 Apesar de reconhecer que é um retrocesso face ao avanço tecnológico, entendo que o combate à tecnologia com tecnologia, poderá um dia ser um fator de descontrolo humano e levar à desumanização, nomeadamente, quando as máquinas se tornarem autónomas (IA). Teoria das Singularidades.

2. Uma Visão Holística

Uma visão holística numa organização é como visionar a criação de uma ponte onde se faça uma travessia harmoniosa, segura e duradoura.

Em tese, acredito[9] que seja possível potenciar esse caminho holístico[10], ponderado e não negligenciando o espaço de conflito[11]. O termo holismo significa "Um todo", é antigo e tem origem do grego "holos" e está implícito em várias conceções filosóficas ao longo de toda a evolução do pensamento humano. A conceptualização holística na sua génese deve ser ampla, interconectada e não reducionista, ou seja, cada parte pertence a um todo, onde os princípios e as leis regentes do todo que se encontram em cada uma das partes, fenômenos ou eventos que se interligam de forma global[12].

Para tal, considero importante exortar valores primordiais, nomeadamente abordar a ética e a moral com um ato formativo nas organizações para o combate a atos ilícitos e realçar a importância destes princípios como o respeito, transparência e compromisso para uma ação global. As empresas estão sujeitas às diversas tentativas e ações ilegais internas ou externas, razão pela qual, devem munir-se e proteger as infraestruturas e informação, tendo em consideração que o trabalhador também é um bem valioso dentro da organização[13].

Assim, um modelo holístico nas estruturas organizacionais para integração da informação entre os departamentos e partilha dessa informação, poderá trazer benefícios na confidencialidade, disponibilidade, integridade e não repudio. Daqui

9 Apresentação SiO, João Lamego «*É necessário os CEO impulsionarem uma linguagem comum, reunir todos os membros nas organizações, de modo, a criar uma cultura aberta sobre os riscos da Cibersegurança*»

10 TEIXEIRA, E. Reflexões sobre o paradigma holístico e holismo e saúde. Rev.Esc.Enf.USP, v.30, n.2, p. 286-90, ago. 1996. «*A holística força um novo debate no âmbito das diversas ciências e promove novas construções e atitudes*»

11 A prevenção: «*A maioria das organizações está mais preparada para responder a ameaças cibernéticas externas, por haver uma maior dificuldade em detetar e prevenir os ataques "insiders"*» (Stroz *et al*, 2016)

12 Segundo Pierre Weil, (1991), "*a abordagem holística propõe uma visão não-fragmentada da realidade onde sensação, sentimento, razão e intuição se equilibram e se reforçam*".

13 Diz Moraes, Terence e Escrivão Filho (2004), «*nenhuma empresa pode escapar dos efeitos da revolução causada pela informação. Dessa forma, deve-se ter consciência de que a informação é um requisito tão importante quanto os recursos humanos, pois dela depende o sucesso ou fracasso das tomadas de decisões diárias*.»

resultaria uma vigilância com compromisso e monitorização da informação para haver mais fiabilidade no cruzamento da interligação dos dados e pessoas, crivando as ações críticas ou suspeitas na esfera da atividade, convergindo para a aquisição de competências e conhecimento para constante melhoramento.

Na experiência das empresas e conforme alguns ilustres autores[14], vivemos dias preocupantes[15], vivemos numa sociedade de informação, moderna e tecnologicamente evoluída onde a manipulação[16] das massas é um alvo com ricochete nos organismos públicos e privados e devem as empresas adequar medidas urgentes, nomeadamente apostar na formação[17].

14 No artigo Ciberespaço: «*Com relação à plataforma virtual em si, observamos diversas opiniões. Por um lado, percebemos preocupações de alguns autores sobre os modos de existência que essa nova realidade também ajudou a criar, como Chauí (2006, 2010) e Bauman (1997, 2000, 2001, 2007,2009), por outro, há os que o defendem, como Lévy (1999), Meira e Mosé (2009), entre vários outros que engrossam a lista de controvérsias sobre essa nova realidade.*», vide: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682015000100012

15 Lê-se no livro verde para a sociedade da informação em Portugal «*Não se pode negar o risco de as tecnologias da informação contribuírem para reforçar o poder dos mais fortes e enfraquecer aqueles que já se encontram numa posição debilitada. Há o perigo dos portugueses ficarem divididos em dois novos grupos: um com acesso aos benefícios da sociedade da informação e do conhecimento e o outro arredado dessa oportunidade em consequência de não poder utilizar, nem ter os conhecimentos necessários, ou a abertura cultural, para aceder a estas novas tecnologias.*», vide: http://homepage.ufp.pt/lmbg/formacao/lvfinal.pdf

16 Como escreveu Avram Noam Chomsky, «*Mas quando você não pode controlar as pessoas pela força, você tem que controlar o que as pessoas pensam, e a maneira típica de fazer isso é através da propaganda (fabricação de consentimento, criação de ilusões necessárias), marginalizando o público em geral ou reduzindo-a a alguma forma de apatia*» (Chomsky, N., 1993)

17 No artigo "a sociedade da informação: possibilidades e desafios", o autor refere «*Nos últimos anos a sociedade vem presenciando inúmeras alterações provocadas pela relação homem, técnica e a tecnologia, o que motivou a importância da preservação e da transmissão do conhecimento. Assim um dos aspetos importantes que merece destaque nesta nova era reside na questão em torno das tecnologias da informação e comunicação (OLIVEIRA; BAZI, 2008). Para que se possa atingir o desenvolvimento da Sociedade da Informação é necessário a integração do acesso a informação capacitando e atualizando os conhecimentos dos cidadãos para que possam competir no mercado de trabalho*.», vide: https://core.ac.uk/download/pdf/268033477.pdf

3. Segurança De Informação

Para aqueles que ocupam a posição de decisor seja no sector privado ou público, independentemente do "ramo do negócio" ou da "área de mercado", a obtenção da informação para a decisão e estabelecimento das estratégias, é absolutamente vital[18], onde a inviabilidade e o acesso à mesma pode comprometer com consequências desastrosas uma organização.

A segurança de informação[19] passa a ter uma relevância no mundo dos negócios, independentemente do setor um objetivo claro para encontrar soluções que proteja os dados das empresas, equipamentos e bens.

A informação é atualmente no mundo organizacional um produto valorizado, necessário e gerado de forma sistémica do qual estamos dependentes, e deve ser[20]: Confidencial, Disponível, Integro e não livre do repúdio.

No artigo do *The New York Times*, Wurman **(1989)**, escreveu: *«Um dia da semana contém mais informações do que um mortal comum poderia receber durante toda a vida na Inglaterra no século XVII; nos últimos 30 anos produziu-se um volume maior de informações novas do que nos 5.000 anos precedentes. Nesse contexto, pode-se afirmar que "o conhecimento é 'moeda' de nosso tempo, e a velocidade de mudanças é a 'taxa de inflação'". Quanto mais alta for essa taxa, mais rapidamente essa moeda perde seu valor. (WURMAN, 1989, p. 32).»* Apesar de já se terem passados trinta e dois anos desde a visão de Wurman, de facto, nos dias atuais onde a informação pode ser disponibilizada de forma incontrolada, qual é a fonte do nosso conhecimento e em que circunstancias?

É indispensável as organizações identificarem a relevância da sua informação e da "Joia da Coroa", de forma, a estruturar de forma holística e ponderada, por

18 Para Beal (2005, p.71) a Segurança de Informação é "*o processo de proteger a informação das ameaças, para garantir a sua confidencialidade, disponibilidade e integridade*".

19 A informação existente deve em qualquer formato ser protegida contra o acesso por pessoas não autorizadas (confidencialidade), disponível 24h (disponibilidade), ser confiável (integridade). O não-repúdio - Garantir que qualquer acesso, visualização ou modificação, seja identificado e por isso não possa ser negado.

níveis de permissão, importância, valor e decisão para que seja possível identificar quais os recursos afetos à gestão, manutenção e sua proteção.

A visão holística tem como base e pilar a importância da aquisição de competências e conhecimento, assim, revejo esta ideia no autor (ALVARENGA NETO, 2002), que refere *«Uma gestão voltada para o conhecimento é aquela capaz de estabelecer uma visão estratégica para o uso da informação e do conhecimento, promover a aquisição, criação, codificação parcial e transferência de conhecimentos tácitos e explícitos, estimular e promover a criatividade, a inovação, a aprendizagem e a educação continuada, além de propiciar um contexto organizacional adequado.»*

É inequívoco que atualmente vivemos num mundo interconectado, onde o fluxo de dados e informações atingem uma velocidade vertiginosa de produção e reprodução, de tal modo, que as empresas e pessoas começam a ter dificuldade na gestão dessa mesma informação. O investimento para proteção do "*asset*" é um fator importante, quantas empresas já foram atacadas julgando que tinham a vanguarda da tecnologia na defesa cibernética (com investimentos de milhares de euros ou dólares) e quantos espaços físicos já foram penetrados apesar da alta segurança.

A propagação e a crescente dependência das tecnologias e a sua interconetividade, no uso intensivo de *softwares* têm grandes desvantagens relativamente à Cibersegurança, no entanto, existem sempre vulnerabilidades[21] apesar das tentativas de proporcionar maior eficiência, segurança e redução do erro humano, independentemente da invencibilidade dos sistemas.

Para assegurar um bom sistema de informação as estruturas organizacionais devem consciencializar-se para as práticas de Ciberhigiene, substanciada na formação e constante atualização.

21 Conforme o autor Miguel Ángel Mendoza, no artigo *welifesecutiry*: «*As vulnerabilidades são um dos elementos que são frequentemente identificados nos incidentes de segurança e, juntamente com outras ameaças, como exploits ou malwares, tornam-se um risco latente. Em 2017, as vulnerabilidades relatadas atingiram seu máximo histórico, ultrapassando os registos de anos anteriores. As vulnerabilidades identificadas como críticas também atingiram seu pico no ano que terminou*.»
vide em: https://www.welivesecurity.com/br/2018/01/04/vulnerabilidades-aumentam-em-2017/

Claramente tudo assenta nas metodologias[22], regras de segurança, processos, identificação de "insiders" ou "outsiders", minimizar as dependências digitais, inventariar as tecnologias de software, hardware e comunicações, políticas de segurança, backups controlados e vigiados, acessos restritos nos espaços físicos e digitais sabendo que nunca será possível estar totalmente protegido[23].

A implementação da cultura "defesa organizacional - *Elo Vigilância ativa*", deverá ser iniciada nos diretores que normalmente não têm conhecimentos e sensibilidade para questões de segurança e da Cibersegurança. As administrações têm um papel basilar na tomada decisão para formar e alertar para as diversas ameaças (Segurança física e no Ciberespaço), dotando os quadros de direção formando a coluna estrutural na defesa.

A formação e o plano de resposta a incidentes como a deteção e analise, contenção, erradicação, e recuperação no após incidente é fundamental. Dever-se-á ter presente que as organizações são vulneráveis e lidam com ameaças internas e externas, onde as ameaças externas são mais difíceis de detetar e prevenir (ataque cibernético) e as ameaças internas podem ser mais vigiadas consoante as políticas de segurança e permissão. Pode haver pequenos incidentes a grandes incidentes, no limite, poderá ocorrer uma paralisação, interrupção parcial ou total da empresa por roubos, danos ou chantagem. Podemos caracterizar e descrever o ciberterrorismo como um conjunto de atos que vão desde o acesso ilícito a identidades de pessoas, ao acesso ilícito, à alteração de informação, à destruição de informação valiosa, para além da disrupção de serviços[24].

Tendo em consideração o contexto apresentado, a Comissão Europeia[25] tem fornecido diretivas e orientações para nortear os Estados-Membros (EM) e

22 Em tese, pressuponho um trabalho holístico - V*ia na defesa ativa numa organização, Elo Vigilância ativa. (EVA)*
23 A análise de risco é um processo importante para identificar os ativos, os riscos desses ativos, criar procedimentos para mitigar os riscos para esses ativos.
24 Inspirado no artigo do Rogério Bravo, Inspetor-Chefe da PJ, no artigo espectro de conflitualidade nas redes de informação.
25 Os regulamentos e as decisões são diretamente aplicáveis em toda a UE na data da sua entrada em vigor. As diretivas devem ser transpostas para o direito nacional pelos países da UE. A Comissão deve verificar se a legislação europeia é aplicada corretamente e no prazo previsto para o efeito e tomar medidas se tal não for o caso.
Vide em: https://ec.europa.eu/info/index_pt

desenvolverem capacidades e políticas públicas de Cibersegurança, das quais se destaca:

- Recomendação R (89)9 - *Computer-Related* crime (Recomendação na origem da primeira 'Lei da criminalidade informática', a Lei109/91, 17AGO);
- ETS (*European Treaty Series*) 185, ou CiberConvenção ou Convenção de Budapeste;
- ETS 190 – Terrorismo;
- Decisão Quadro 2002/C 203 E/16 CE 2005/222/JAI; Directiva 2013/40/UE do Parlamento e do Conselho de 12 de agosto de 2013 - ataques a Sistemas informáticos;
- Decisão Quadro 2006/960/JHA, de 18 dezembro - intercâmbio de Informações Diretiva UE 2016/1148 de 6JUL do Parlamento Europeu e do Conselho – 'Diretiva NIS'20;
- Regulamento UE 2016/679 do Parlamento Europeu e do Conselho (RGPD) Diretiva EU 2015/2366 – Serviços Pagamentos eletrónicos ("PSD2");
- Regulamento 2016/680, 27ABR do Parlamento Europeu e do Conselho proteção dados pessoais para prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.
- Regulamento (UE) 2019/881 do Parlamento Europeu e do conselho de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da Cibersegurança das tecnologias da informação e comunicação.

Em relação à legislação nacional, destaco os seguintes diplomas legais[26]:

- Lei 109/09 15SET – Lei do cibercrime;
- Lei 58/19 08AGO – Lei de execução do RGPD;
- Lei 59/19 08AGO – Dados pessoais para efeitos de investigação criminal;
- Decreto-Lei 252/94 20OUT – Proteção do software.
- DL n.º 63/85, de 14 de MAR - Código Direitos do Autor e Direitos Conexos (CDADC)

26 Incluindo o Código de Processo Penal Português (CPP), DL n.º 78/87, de 17 de fevereiro 1987.

- Lei 41/2004 18AGO - proteção de dados pessoais nas telecomunicações
- Lei 46/18 13AGO – Lei da Cibersegurança
- Lei 32/2008 17JUL – salvaguarda de dados de tráfego

Ainda respeitante à segurança de informação[27], são identificáveis em qualquer organização várias vulnerabilidades, podendo ser da seguinte natureza:

- **Natural:** Fenómenos da Natureza
- **Tecnológicas:** Em redes, computadores, Controlos de acesso físico
- **Físicas:** O local dos computadores e periféricos, ausência de energia elétrica, permissões acesso local, armazenamento documentos
- **Humanas:** Envolve o fator humano, considerada a mais difícil de avaliar, por envolver características psicológicas, emocionais, socioculturais, que variam de pessoa para pessoa, pode ser devido: falta de formação, qualificação, ambiente organizacional inapropriado para desenvolvimento das atividades.

Conforme referido por José Manuel Gaivéo[28] «*A Vulnerabilidade pode ser entendida como uma fraqueza ou falha num sistema ou mecanismo de proteção que expõe ativos de informação a ataques ou danos [Pfleeger and Pfleeger 2003, Whitman and Mattord 2005], como uma fraqueza num sistema, aplicação ou infraestrutura, que pode ser explorada para violar a integridade do sistema [Peltier 2001], ou ainda como uma fraqueza de um ativo ou grupo de ativos que podem ser explorados por uma ou mais ameaças [ISO 2004].*»

Sem dúvida que é necessário defender os nossos ativos e identidades conhecendo as ameaças, sendo uma preocupação das organizações e das pessoas. Devemos tomar diligências para proteger os "Valores", sendo um tema[29] preocupante, urgente e prioritário, que não posso deixar de utilizar um aforismo, **"A**

27 Segundo Sêmola (2003, p. 9) define a Segurança da Informação como «uma Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade».
28 Tese Doutoramento "*As Pessoas nos Sistemas de Gestão da Segurança da Informação*".
29 Um tema que tem sido alertado pelo União Europeia, Governo português, autoridades competentes, (CNCS), investigadores, docentes, jornalistas e queixosos.

Cibersegurança começa em cada um de nós", portanto, a resposta ao combate é de todos nós e não apenas dos Estados e Organizações.

Nesta ocasião, as organizações e pessoas devem ser sensibilizadas para uma correta gestão dos seus dados, identidade e procurar como proceder à implementação de um conjunto de medidas preventivas, adotar e reforçar as boas práticas e acesso à informação, tais como:

- Ter cuidado e atenção relativamente aos sites que se visita;
- Avaliar e Validar a fiabilidade dos e-mails que se recebe antes de os abrir;
- Ter muita atenção ao tipo de links que os seguem;
- Ter cuidado com mensagens atrativas e compras promocionais;
- Optar pela autenticidade biométrica e de passwords se possível complexa, fazendo manutenção da mesma temporariamente;
- Manter equipamentos e aplicações atualizadas e usar conexões confiáveis (VPN);
- Criar o hábito de efetuar cópias de segurança e mantê-las "isoladas" e seguras
- Ficar atento a notícias: https://www.cncs.gov.pt/
- Notificar Incidentes: https://www.cncs.gov.pt/certpt/notificar-incidente/

Um Incidente pode ser definido como uma ocorrência que coloca em risco a confidencialidade, integridade ou a disponibilidade dum Sistema de Informação ou dos seus processos, armazenamento ou transmissão, ou que constitua uma violação ou ameace vir a violar as políticas de segurança, procedimentos de segurança ou as políticas em vigor. (NIST[30] N. I., 2013).

30 National Institute of Standards and Technology

4. Fundamentos Da Ética E Honra Na Estrutura Da Organização

Nos capítulos anteriores abordei a forma como gostaria de introduzir na estrutura organizacional o conceito "holismo" e a visão como se poderá encaminhar em benefícios no ceio do trabalho[31], onde cada um faz parte de um todo.

Atualmente a maior vulnerabilidade e ameaça é a ação humana, contudo num futuro preocupante pela alta tecnologia[32], onde o desenvolvimento da inteligência artificial, *machine learning* e *Cyborgs* já não são uma miragem, poder-se-á enfrentar outros riscos.

Quem saberá se as próprias máquinas adquiram capacidade de se construírem, reconfigurarem, autonomizarem e se tornarem num agente decisor movido pela segurança, aprendizagem e autoprogramação para a sua sobrevivência.

Em reflexão julgo que é fundamental desenvolver fundações mais fortes mais do que nunca, a formação é essencial pois vivemos num mundo onde o teste aos nossos limites são uma constante, precisamente na esfera da ausência da ética, moral e Honra.

A ética no seu sentido etimológico é a palavra oriunda do grego "*ethos*" e define-se por duas formas (Trigo (1999, p.225; Dias, 2004, p.85). A primeira, "*ethos*", refere-se ao modo de ser, ao carater, à realidade interior donde provêm os atos humanos. A segunda *éthos*, indica os costumes, os hábitos ou o agir habitual; atos concretos que indicam e realizam o modo de ser do indivíduo.

As morais, pretendem ditar como pelas regras dos seus respetivos grupos, os indivíduos deverão comportar-se, ou deverão ser[33].

31 Maria Olívia Dias, refere «*a ética e as organizações, tornam-se indissociáveis estando diretamente ligadas a relações, a comportamentos, que nas ciências sociais, não esquecendo a sua dimensão teórica ou cognitiva, assumem medidas que contemplam as observações empíricas.*»

32 De acordo com o mito da singularidade, adquirimos mais do que nunca legitimidade para opinar neste tema controverso, onde a "promessa" da «transhumanidade» poderá tornar-se numa arma perigosa, para obter poder e conhecimento.

33 CUNHA, Paulo Ferreira da – Filosofia Jurídica Prática, pp.47-48

O autor Bernardes, Marcelo DI Rezende, resume bem a diferença da ética e moral «[…] pode acontecer de várias maneiras: Ética é princípio, moral são aspectos particulares de determinado tipo de conduta; ética é permanente, moral é temporária; a Ética possui a propriedade da universalidade enquanto a moral é restrita à dada cultura; ética é regra, moral é prática de tal regra; ética é teoria, moral é prática desta teoria.»

A ética e moral andam de mãos dadas, sendo conceitos interligados e verificáveis nas ações diárias.

São valores, regulamentos, normas, regras e leis por onde se regem as pessoas na sociedade e respetiva conduta nas organizações. Define-se como Honra[34] no antigo, como princípio de comportamento no ser humano que age baseado em valores fortes e bondosos, como a honestidade, a dignidade, a bravura e outras características que são consideradas socialmente virtuosas[35]. O autor Pedro Pais de Vasconcelos[36], refere o seguinte: «(…) *o direito à vida, ou à honra, ou à integridade física, ou à privacidade, ou à imagem, […] não constituem direitos subjetivos autónomos mas, antes poderes jurídicos que integram o direito de personalidade do seu titular*» o autor ainda realça a defesa da honra referindo-se como uma mais importantes concretizações do direito de personalidade, refere mesmo que a honra é «(…) um preciosíssimo bem da personalidade […] todas as pessoas têm direito à honra pelo simples facto de existirem, isto é, de serem pessoas. A honra ao longo dos tempos pode sido oprimida, perjurada e tentada ao esquecimento pelo indivíduo, mais no íntimo o bravo nunca a perde[37], cessará no dia da sua morte.

Os fatos históricos são claríssimos e cada época ficou marcada pela natureza humana e o seu impacto, perscrutadas e dessecadas até ao momento do sacrifico,

34 Código de Honra dos Samurais – "*Bushido*" – vide em: https://kyokushinkaikan.com.br/codigo-de-honra-dos-samurais-bushido/

35 O Samurai que surgiu no Século VIII, "Aquele que serve" na tradução de Samurai para o português. A preservação da Honra estava acima de tudo, caso a mesma fosse manchada e não conseguisse limpá-la, este realizava o ritual suicida de "*Seppuku*".

36 VASCONCELOS, Pedro Pais de Vasconcelos – Direito de Personalidade. Op. Cit.

37 Cito o art. 70º, nº1, do Código Civil tutela a personalidade como direito absoluto de exclusão, na perspetiva do direito à saúde, à integridade física, ao bem-estar, à liberdade, **ao bom nome e à honra**, que são os aspectos que individualizam o ser humano, moral e fisicamente e o tornam titular de direitos invioláveis.

selados os lábios em cima do altar e preservemos a Honra, do antigamente ao agora, apesar dos momentos de aflição, angústia, opressão, medos, doenças e guerras.

O código de Honra apela ao nosso mais profundo e sentido de respeito, lealdade, coragem, veracidade, decência e dignidade, especialmente agora, que o Mundo *Ciber* irá contribuir muito para a desumanização[38].

Para Manuel Castells, «*a internet/web e a sociedade em rede eram o resultado de uma encruzilhada insólita entre a ciência, a investigação militar e a cultura libertária* (2004, p. 34).», segundo o autor, existe a preocupação e apercebemos que a internet e sociedade em rede ficarão subjugadas aos principais vetores da revolução digital.

O mundo digital veio para ficar e as tecnologias da informação e comunicação são o futuro e partilho a opinião que trazem grande facilidade no acesso à informação ao dispor da educação, novo paradigma de aprendizagem, investigação, saúde, partilha da informação, mas confesso alguma reserva e preocupação na dependência para atos de decisão.

Outra preocupação no mundo digital é a forma como convergimos para a obtenção do conhecimento, será que estamos a ampliar o nosso conhecimento[39] e intelecto?

38 "*Na condição fragmentária e acidentada do self enquanto corpo incessantemente possuído e despossuído, conectado e desconectado, pelos dispositivos da sociedade globalizada, adivinha-se o mise en abîme de um sujeito em vertigem, fragmentado até ao infinito nesse espaço que lhe permite ser quantos de si desejar sob o anonimato de máscaras textuais e imagéticas*.", por Catarina Moura (2002): Vertigem (da ausência como lugar do corpo), vide em: www.bocc.ubi.pt

39 Textos Filosóficos. Vol. II. Fernando Pessoa. (Estabelecidos e prefaciados por António de Pina Coelho.) Lisboa: Ática, 1968. - 223., «*Todo o conhecimento vem dos ou pelos sentidos; porém não sabemos quantos são os sentidos (quantos sentidos há). Sentidos chamamos nós àqueles dispositivos da mente pelos quais toma conhecimento (recebe uma impressão de que qualquer coisa existe, e de que essa coisa apresenta determinado aspecto)*.»

5. Norma NP ISSO/IEC 27001:2013

Na temática a Segurança da Informação parece-me importante abordar o Sistema de Gestão, mais precisamente, a norma NP ISO/IEC 27001:2013, que tem como princípio a implementação de processos e controlos com o objetivo de mitigar e gerir o risco da Organização em relação à segurança da informação.

O foco é na preservação da fiabilidade e segurança dos ativos de informação, em relação à confidencialidade, disponibilidade, integridade e acrescento o não repudio, protegendo-os contra as ameaças e vulnerabilidades.

Os requisitos do sistema de gestão da qualidade especificados na norma ISO 9001:2015 adota a abordagem por processos, que incorpora o ciclo PDCA, conforme se ilustra na figura abaixo.

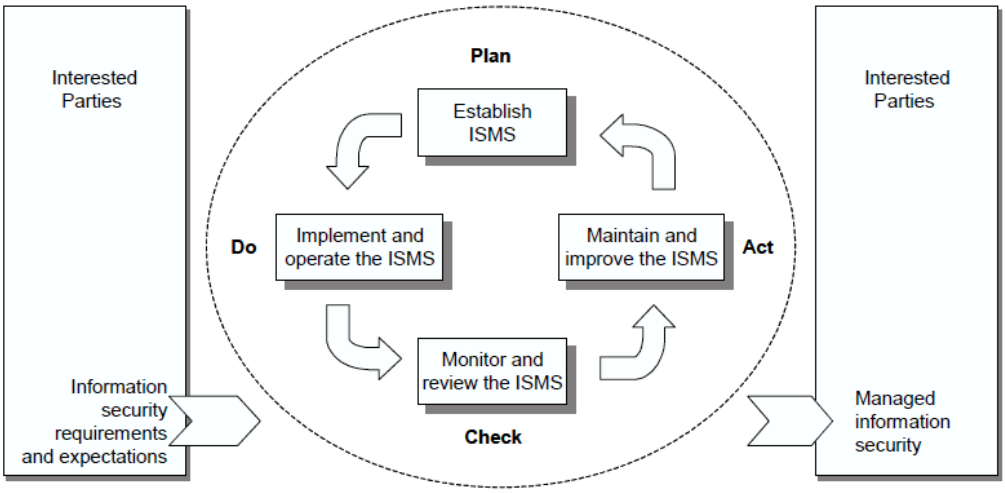


Figure 1 — PDCA model applied to ISMS processes

Figura 1[40] – Ciclo PDCA (*Plan-Do-Check-Act*)

40 A figura 1, como base a ISO/IEC FDIS 27001:2005.

Respeitante à ISO 27001[41], existem controlos obrigatórios que são abordados desde o capítulo 4 ao 8 da norma, para que os sistemas de segurança das organizações estejam realmente em conformidade com a ISO 27001, nomeadamente:

- Capítulo 4. (*Information security management system*) - Sistema de Gestão de Segurança da Informação
- Capítulo 5. (*Management Responsability*) - Responsabilidade de Gestão
- Capítulo 6. (*Internal ISMS audits*) - Auditorias internas de um ISMS
- Capítulo 7. (*Management review of the ISMS*) - Gestão de revisão do ISMS
- Capítulo 8. (*ISMS improvement*) – Melhoramento do SGSI
- *Annex A* (*Control objectives and controls*) – Anexos A – Objetivos de Controlo e Controlo

✓ Política de Segurança; Organização de informações de segurança; Gestão de segurança dos recursos humanos; Segurança física e ambiental; Gestão de comunicações e operações; Controlos de acesso; Aquisição de sistemas de informação, desenvolvimento e manutenção; Gestão de incidentes de segurança; Gestão continuada; Reporte e *Compliance*.

A ISO 27001 é um guia que norteia qualquer organização na implementação de um sistema de gestão que visa assegurar e proteger a segurança de informação e respetiva informação.

41 Excerto retirado da ISO 27001 «*1.2 Application, the requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard. Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such*
exclusions do not affect the organization's ability, and/or responsibility, to provide information security that
meets the security requirements determined by risk assessment and applicable regulatory requirements. »

6. Conclusão

Em jeito de conclusão parece-me importante destacar que estamos submersos numa panóplia de tecnologias existentes no mercado, com menor ou maior acessibilidade, eficiência, proteção ou avanço tecnológico, mas indubitavelmente leva-me à reflexão se devemos ou não estar subjugados às gigantescas tecnológicas e qual a barreira da nossa Liberdade.

A reflexão poderá ser ainda mais pervertida, queremos nós ficar dependentes das grandes tecnológicas sabendo que influenciam e manipulam o poder político, e qual é a barreira e a imparcialidade dos decisores que atuam na governação dos estados-nação.

O nosso dia a dia é assente nas tecnológicas e nas redes de comunicação, somos transportados para um globo digital onde o futurismo já é o presente onde enfrentamos desafios, riscos e oportunidades, mas deveremos ter em mente que tais mudanças poderão transformar-se num vórtice de potencialidades que convergem para uma catástrofe social.

É verdade que vivemos numa época demasiado avançada para questionar ou refletir no absurdo, mas é intrínseco ao Homem livre fazê-lo, é o momento exato para questionar e tomar consciência aonde estamos e para onde queremos, e qual o papel das Tecnologias no nosso legado e se estamos dispostos a tal determinismo.

Posso proferir uma opinião demasiado leiga ou questionável, mas procuro suscitar a transformação alquímica de como seria enfrentarmos um novo mundo dando num passo atrás, como seria desligarmos as máquinas e a *internet*, qual a nudez das tecnologias perante tal observância humana, que reconheço insana na atualidade.

Deambulando sem retrocesso, a solução passará por capacitarmo-nos com mais tecnologia, onde deverá ser salvaguardado o conhecimento, identidade e exortar o sentido ético, moral e com honra combater as vulnerabilidades holisticamente nas organizações e na sociedade, com esperança e perseverança em alcançarmos um futuro melhor para os nossos filhos, nosso Legado.

Bibliografia e Fontes

ARTICLE 19. USA must respect international standards on protection of whistleblowers.

Disponível:http://www.article19.org/resources.php/resource/37133/en/usa-must-respectinternational- standards-on-protection-of-whistleblowers.

A arte da Guerra – SUN TZU, Bertrand Editora, 2009

Cibersegurança, Visões Fundamentais Harvard Business Review, CoAtual Conjetura Editora, 2019

Castells, Manuel, A SOCIEDADE EM REDE. A Era da Informação: Economia, Sociedade e Cultura,1999

CANELA, Guilherme; NASCIMENTO, Solano. Acesso à informação e controle social das g20 anti-corruption action plan protection of whistleblowers.

Cibercultura / Pierre Lévy; tradução de Carlos Irineu da Costa, São Paulo: Ed. 34, 1999, 264 p.

CHOO, Chun Wei - A Gestão de Informação para a organização inteligente: A arte

de explorar o meio ambiente. 2003.

CHOO, Chun Wei - Information Management for the Intelligent Organization. 1998.

Cabral, R. (2000). Temas de ética, Braga: UCP:

Decio, Z. (2002). Organização Ética: um ensaio sobre comportamento e estrutura das organizações. Acedido a 2 de fevereiro de 2014. Disponível em http://www.scielo.br/pd/rac/v6n2/v6n2a 08.pdf

ISO/IEC 27001 - Information security management systems - Requirements. 2005.

Llufríu, M., "Impacte das Tecnologias de Informação e Comunicação na Sociedade do Conhecimento", in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António

Serrano Carlos Zorrinho (Editores), Sistemas de Informação Organizacionais, Edições Sílabo, 2005, p.95-112.

LÉVY, Pierre. O que é virtual? São Paulo: Editora 34, 2007.

Lourenço, R.T. e O'Neill, H., "As Tecnologias de Informação e Comunicação na Gestão Empresarial e o papel dos Recursos Humanos na sua Potenciação", Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de novembro de 2002.

MENDEL, Toby. Liberdade de informação: um estudo de direito comparado. 2 ed. Brasília: UNESCO, 2009.O'NEILL, Ben. Edward Snowden e a ética da delação.

The ethics of State secrecy.: http://mises.org/daily/6475/The-Ethicsof-State-Secrecy.

Novais, Rui Alexandre "Media e (Ciber)Terrorismo", http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problem%C3%A1tica-da-ciberseguran%C3%A7a-e-os-seus-desafios.pdf

Nunes, P. (2007). Conceito de organização.

Rego, A. (2000). Comportamentos de cidadania organizacional – diferentes padrões reativos às perceções de justiça. Organização e Trabalho

Rego, A. Moreira, J. M. & Sarrico, C. (2003). Gestão ética e responsabilidade social das empresas, S. João do Estoril: Principia.

Rogério Bravo, Inspector-Chefe da Polícia Judiciária, Do espectro de conflitualidade nas redes de informação, 2010

Rogério Bravo, Inspector-Chefe da Polícia Judiciária, Segurança da informação, CiberSegurança e Cibercrime: contributos para um alinhamento de conceitos, v7

Santos, A.M. (2016). "Segurança e Globalização: A Perspetiva dos Estudos Críticos de Segurança".

SOARES, Magda. Novas práticas de leitura e escrita: letramento na cibercultura. Educ. Soc. [online]. 2002. v. 23, n. 81, p. 143-160

VASCONCELOS, Pedro Pais de Vasconcelos – Direito de Personalidade. Op. Cit.

Websites:

http://www.transparency.org/whatwedo/pub/international_principles_for_whistleblower_legislation.

https://www.unidosparaosdireitoshumanos.com.pt/course/lesson/background-of-human-rights/the-background-of-human-rights.html

http://www.unesco.org/new/en/social-and-human-sciences/themes/most-programme/

https://ec.europa.eu/digital-single-market/en/news/network-and-informationsecurity-directive-co-legislatorsagree-first-eu-wide-legislation;

https://cio.com.br/tendencias/9-ciberameacas-que-rondarao-as-empresas-em-2020/

http://www.cio.pt/2020/06/22/vulnerabilidades-das-organizacoes-aumentaram-60-no-periodo-de-confinamento/

https://www.itchannel.pt/news/seguranca/especialistas-preveem-vulnerabilidade-recorde-em-2020

http://bocc.ubi.pt/pag/fidalgo-moura-devir-inorganico.pdf

http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0003-57320130002000001

https://kyokushinkaikan.com.br/codigo-de-honra-dos-samurais-bushido/

https://repositorio.uniceub.br/jspui/bitstream/235/9932/1/20400835.pdf

CYBERLAW by CIJIC

O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM *CASE STUDY.*

MELISSA ADRIANA GONÇALVES DE SOUZA*

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestranda em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

O presente estudo traz à reflexão os impactos do fator humano na segurança da informação nas organizações, tanto sob o aspecto positivo quanto no negativo. A problemática que se quis apresentar aqui não é apenas a fraqueza ou a falha humana, mas também o olhar curioso e crítico que apenas uma pessoa poderia ter sobre determinada operação ou processo dentro de uma empresa. A proposta do tema tem como origem o caso ocorrido com o Banco HSBC após a aquisição do Banco Bital (México) dando-se foco na contribuição humana não apenas na concretização da fraude, mas principalmente na sua resolução, o que nos leva a concluir que a segurança da informação nas organizações tem grande relação com pessoas: O fator humano.

Palavras-Chave: Informação, segurança da informação, fator humano, engenharia social e vulnerabilidades.

ABSTRACT

The present study brings to reflection the impacts of the human factor on information security in organizations, both from a positive and a negative aspect. The problem that we´d like to present here is not only about human weakness or failure, but also the curious and critical look that only one person could have on a particular operation or process within a company. The focus of this study was based on the case that occurred with HSBC Bank after the acquisition of Bital Bank (Mexico), focusing not only on human contribution to prevent fraud, but mainly in its resolution, which leads us to conclude that information security in organizations has a strong linked with people: the human factor.

Keywords: Information, information security, human factor, social engineering and vulnerabilities.

1.INTRODUÇÃO

O tema proposto é uma junção de assuntos relativos ao conteúdo aprendido nas aulas de Segurança da Informação na Organizações (SIO) ministradas pelo Professor Dr. Gonçalo Sousa no curso de Mestrado em Segurança da Informação e Direito no Ciberespaço (MSIDC) e da experiência vivenciada na minha atuação profissional junto ao banco HSBC Bank Brasil S.A. entre os anos de 2014 a 2016.

Em 2010, o banco HSBC (subsidiária do México) foi acusado pelo senado norte americano por possuir um sistema de monitoramento e controle de operações financeiras pouco eficiente na prevenção à lavagem de dinheiro, indicando que isso acarretou na exposição do sistema financeiro dos Estados Unidos (EUA) a uma ampla rede de lavagem de dinheiro, tráfico de drogas e financiamento ao terrorismo. Ainda, o senado americano afirma que foram mais de 28 mil transações irregulares realizadas pelo HSBC durante o período de 2001 a 2008. Há indicação que o Irão estaria envolvido em 25 mil dessas movimentações que envolveram cerca de 19,4 mil milhões de dólares.

Em 2012, o HSBC fez um acordo com o departamento de Justiça dos Estados Unidos, comprometendo-se a pagar aproximadamente dois mil milhões de dólares, bem como fazer uma carta de confissão assumindo os erros cometidos pelo banco na falta de monitoramento adequado das suas operações, e também firmou o compromisso público de reforçar seu sistema de alertas e de investigações internas, não podendo pelos próximos 5 anos (2012 a 2017) incorrer em nova fraude de qualquer de suas filiais sob pena de perder a licença de atuar como instituição financeira nos Estados Unidos[1].

A questão que se quer trazer a análise neste trabalho é como o fator humano pode interferir na segurança da informação nas organizações tanto no aspecto positivo quanto no aspecto negativo. A problemática que se quer abordar não é apenas a fraqueza ou a

1 Disponível em: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations acesso em 07/01/2021.

falha humana, mas também o olhar curioso e crítico que apenas um humano poderia ter sobre determinada operação ou processo dentro de uma empresa.

Importante dizer em primeiro lugar, e isso será abordado de forma mais aprofundada ao longo deste trabalho, que o fator humano foi ao meu ver, no caso do HSBC, a peça chave tanto no que se pode dizer do aspecto negativo, ou seja, na concretização das fraudes, mas também no apontamento da questão e da resolução do problema, ainda que de forma a expor um instituição a um risco reputacional mundial. Em segundo lugar é salutar destacar que os fatos aqui apresentados são públicos e não estão amparados por nenhuma forma de sigilo, de forma que não há óbice em expor tais acontecimento neste estudo, além de vários jornais ao redor do mundo terem publicados os fatos acorridos, o caso virou um documentário da *Netflix*[2].

2 A *Netflix* reconta a história da fraude no HSBC no documentário intitulado "Na Rota do Dinheiro Sujo", episódio: "O banco dos carteis". Para recontar a história do banco a Netflix convidou várias pessoas que, na época, participaram de alguma forma com a investigações dos fatos, como por exemplo: 1) Everett Stern, ex-funcionário do HSBC (Compliance Officer do HSBC entre os anos de 2010 e 2011); 2) Anabel Hernandéz, jornalista investigativa e escritora; 3) William Ihenfeld, Procurador-geral em Virginia Ocidental (2010 a 2016); 4) Brett Wolf, Jornalista correspondente sobre Prevenção à lavagem de dinheiro para o Thomson Reuters; e 5)Matt Taibbi, jornalista correspondente da Rolling Stone magazine.

2. Segurança da Informação nas Organizações

Quando falamos em segurança da informação nas organizações inevitavelmente vem-nos à mente a ISO 27001, que é uma norma padrão internacional de referência no tema. Segundo o portal informativo da ISO 27001[3] a adesão da norma "*serve para que as organizações adoptem um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação*".

Sabemos que a segurança da informação nas organizações envolve um conjunto de requisitos, processos e controles para mitigar riscos e isso impacta de várias formas dentro de uma empresa: como as telecomunicações, segurança aplicacional, proteção do meio físico, recursos humanos, continuidade de negócio, confiabilidade da marca, licenciamento, etc.[4].

Conceitualmente a segurança da informação está baseada na tríade "CIA" (sigla em inglês para *Confidentiality*, *Integrity* and *Availability*[5]): confidencialidade, integridade e disponibilidade das informações.

A confidencialidade está relacionada aos mecanismos de segurança que são adotados pela empresa para evitar que informações sensíveis sejam expostas, seja por meio de ciberataques, espionagem, fraudes, ou quaisquer outras práticas indevidas. Já a integridade refere-se à confiabilidade das informações e sistemas no decorrer do ciclo de vida dos dados, é a manutenção do armazenamento dos dados sem que qualquer interferência possa corrompê-los ou danificá-los. Enquanto que a disponibilidade está diretamente relacionada ao acesso às informações, ou seja, as informações devem estar disponíveis para serem consultadas a qualquer tempo por seus colaboradores, por exemplo[6].

3 Disponível em: https://www.27001.pt/iso27001_2.html acesso em 20/12/2020.
4 Disponível em: https://www.27001.pt/index.html acesso em 20/12/2020.
5 Disponível em: https://www.techrepublic.com/blog/it-security/the-cia-triad/ acesso em 21/12/2020.
6 Disponível https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao.

Nesta perspectiva podemos observar que é notória a importância da segurança da informação para que as organizações mantenham seus sistemas protegidos, não apenas pela relevância das informações internas ou de seus clientes, ou ainda pela questão reputacional, mas principalmente para a continuidade dos seus negócios.

Sabemos também que há várias formas de ataque à segurança da informação de uma organização como por exemplo: vírus[7], vulnerabilidades dos *softwares*[8]; ciberataques[9], *fishing*[10], *spam*[11], engenharia social[12], entre outros.

Para resumir:

> "*A segurança de informação é o processo de proteger a informação de diversos tipos de ameaças internas e externas que coloquem em risco a continuidade do negócio e o retorno dos investimentos feitos. A adopção e implementação de um sistema de segurança é uma decisão particular de cada organização que é influenciada pelas necessidades e objectivos da empresa, requisitos de segurança, capital investido, tamanho e estrutura da organização. Assim sendo deve ser feita uma*

7 CORTEZ, Igor Siqueira e KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. 2021, pág. 759. Disponível em: https://www.researchgate.net/profile/Luis_Kubota/publication/259360942_Contramedidas_em_seguranca_da_informacao_e_vulnerabilidade_cibernetica_evidencia_empirica_de_empresas_brasileiras/links/00b7d52b31b2030da9000000/Contramedidas-em-seguranca-da-informacao-e-vulnerabilidade-cibernetica-evidencia-empirica-de-empresas-brasileiras.pdf. Acesso em 08/12/2020.

8 Idem pág. 3.

9 Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo. 2015 pág. 42. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/15403/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf acesso em 12/12/2020.

10Miller, Andrew. Phishing: An Insidious Threat to Financial Institutions. 2006. https://www.bankinfosecurity.com/phishing-insidious-threat-to-financial-institutions-a-121 acesso em 22/12/2020.

11 SILVA, Thiago Domingos de Souza. Segurança na Internet: Qual a nossa Vulnerabilidade? Pág 2. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2603/2551 acesso em 07/12/2020

12 Engenharia social definição: "*Any act that influences a person to take an action that may or may not be in their best interest.*" *We have defined it in very broad and general terms because we feel that social engineering is not always negative, but encompasses how we communicate with our parent, therapists, children, spouses and others*.
Tradução livre: "*Qualquer ato que influencie uma pessoa a realizar uma ação que pode ou não ser de seu interesse". Definimos de uma forma geral porque achamos que a engenharia social nem sempre é negativa, mas abrange a forma como nos comunicamos com nossos pais, terapeutas, filhos, cônjuges e outros*. Disponível em: https://www.social-engineer.org/about/ acesso em 02/01/2021.

> *análise de risco que identifique as potenciais ameaças, apontando soluções que as eliminem, minimizem ou as transfiram a terceiros*"[13].

Ainda, sobre as ameaças internas à segurança da informação há dados estatísticos que mostram que a engenharia social é um dos fatores de risco que afeta mais de metade das violações a dados ocasionadas por ameaças internas:

> "*De acordo com a verizon (2016) foram encontrados indicadores estatísticos interessantes sobre as novas tendências de crimes informáticos, que mostram que a nova geração de ataques está a utilizar o factor humano para desencadear com frequência ataques a TI sem o uso de meios electrónicos*"[14].

Neste estudo o que se quer analisar é o fator humano como decisivo para o sucesso ou para o fracasso dos mecanismos de segurança da informação nas organizações. Para tanto, traz-se a análise o caso do banco HSBC que em 2010 foi acusado pelo senado norte-americano de não ter um sistema interno eficiente no controle das suas operações, acarretando a exposição do sistema bancário mundial à lavagem de dinheiro e financiamento ao terrorismo, e ao tráfico de drogas. Assim, a seguir apresenta-se um breve resumo dos fatos públicos[15] ocorridos naquela instituição financeira.

13 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 12.
14 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 4.
15 Todos os dados ou informações aqui apresentadas foram retirados de fontes públicas de consulta online e gratuita disponível na *internet* e para todas as informações são apresentadas suas fontes de pesquisas em notas de rodapé ou no próprio corpo do texto. Não foram utilizadas informações privilegiadas de dentro da instituição, com exceção da minha percepção pessoal sobre o tempo em que atuei profissionalmente naquela instituição (2014 a 2016) a qual faço menção unicamente no ultimo parágrafo das 'considerações finais' deste trabalho.

3. O *Case Study*

Tudo começou em 2012 quando a subsidiária do banco inglês HSBC (Hong Kong and Shanghai Banking Corporation) sediada no México foi acusada de lavar dinheiro para os cartéis de drogas. Esta foi a conclusão do relatório produzido pelo senado norte americano, que indica que milhares de milhões de dólares oriundo do narcotráfico e do terrorismo foram inseridos no sistema financeiro dos Estados Unidos da América por falha na operação do HSBC.

O senador Carl Levin que presidiu a subcomissão emissora do relatório afirmou que o banco possuía uma cultura "contaminada" e por isso permitiu que clientes recebessem valores de países de origem duvidosas como: Irão, Ilhas Cayman, Arábia Saudita e Síria[16].

Para entendermos como tudo isso aconteceu, é preciso voltar aos anos de 2002 quando o HSBC adquiriu a operação do Banco Bital no México, que na época era considerado o quinto maior banco do México[17] e foi adquirido por 1,14 mil milhões de dólares. O Bital com grande presença no México, principalmente em Sinaloa que é uma região conhecida por produção de narcóticos.

Juntamente com a aquisição das operações do Bital o banco HSBC "comprou" também os funcionários, os clientes e suas contas bancárias. O documentário da *Netflix*[18] que reconta essa história, com a participação de alguns dos personagens que participaram das investigações na época (ex-executivo do banco HSBC, procuradores de justiça e jornalistas investigativos)[19], indica que junto com aquisição o banco comprou inevitavelmente, contas bancarias dos narcotraficantes, bem como colaboradores

16 Disponível em: https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves acesso em 10/01/2021.
17 Disponível em https://www.nytimes.com/2002/08/22/business/hsbc-buying-fifth-largest-bank-in-mexico-for-1.1-billion.html acesso em 10/01/2021.
18 O documentário da Netflix reconta a história da fraude no HSBC: "Na Rota do Dinheiro Sujo" Nome do episódio: "O banco dos carteis".
19 Pessoas que participaram das investigações dos fatos narrados na séria da Netflix (vide nota de rodapé n. 4): 1) Everett Stern, ex-funcionário do HSBC (Compliance Officer do HSBC entre os anos de 2010 e 2011); 2) Anabel Hernandéz, jornalista investigativa e escritora; 3) William Ihenfeld, Procurador-geral em Virginia Ocidental (2010 a 2016); 4) Brett Wolf, Jornalista correspondente sobre Prevenção à lavagem de dinheiro para o Thomson Reuters; e 5)Matt Taibbi, jornalista correspondente da Rolling Stone magazine.

corruptos que “facilitavam” a inclusão do dinheiro oriundo do narcotráfico no sistema bancário. Como o HSBC é um banco mundial, o dinheiro dos carteis passava naquele momento a ser inserido no sistema financeiro mundial.

Os jornais ao redor do mundo começaram a noticiar a falha nas operações do banco:

> “*O banco britânico HSBC expôs o sistema financeiro dos Estados Unidos a uma ampla rede de lavagem de dinheiro, tráfico de drogas e financiamento de terroristas devido ao seu fraco sistema de controle, diz um relatório do Senado dos Estados Unidos que investigou as filiais do banco no país por um ano*”[20].

Em 2010 o escritório regulador do banco federal americano “OCC” (Sigla inglesa para: “*Office of the Comptroller of the Currency*”[21]), solicitou ao HSBC que realizasse maior controle nas suas operações, foi por isso que naquele mesmo ano o HSBC estabeleceu em Delaware/USA um escritório para monitoramento dos alertas das operações financeira.

Importante dizer que nos Estados Unidos está em vigor a Lei do Sigilo Bancário “BSA” (sigla em inglês para *Bank Secrecy Act*), também conhecida como Lei Anti-Lavagem de Dinheiro “AML” (sigla em inglês para *Anti-Money Laundering*), e com isso todas as instituições financeiras com atuação naquele país devem manter registros detalhados e relatar às autoridades nacionais quaisquer atividades suspeitas que possam indicar lavagem de dinheiro ou quaisquer outros crimes que detectem em suas operações.

Fazem parte destes alertas monitorar e impedir operações com empresas, bem como com os países que compõe a lista de restrições do governo norte-americano. O escritório governamental de controle de ativos estrangeiros “OFARC” (sigla em inglês para “*the Office of Foreign Assets Control*") que é uma divisão do Departamento do Tesouro dos Estados Unidos que administra e aplica sanções econômicas e comerciais com base na política estrangeira do país e metas nacionais de segurança contra determinados países e regimes políticos, terroristas, traficantes internacionais de drogas, pessoas envolvidas em

20 Disponível em: https://www.correiocidadania.com.br/colunistas/consciencia-negra/33-artigos/noticias-em-destaque?start=924 acesso em 10/12/2020.
21 Site: https://www.occ.treas.gov/

atividades relacionadas com a proliferação de armas de destruição em massa e outras ameaças à segurança nacional, à política estrangeira ou à economia dos Estados Unidos.

Por isso, algumas sanções se aplicam de forma ampla a determinadas regiões (como Cuba e Irão), enquanto outras são direcionadas e concentradas em pessoas e entidades específicas[22]. Todas as restrições, impedimentos estão disponíveis no site Tesouro Nacional Norte-americano[23] para consulta.

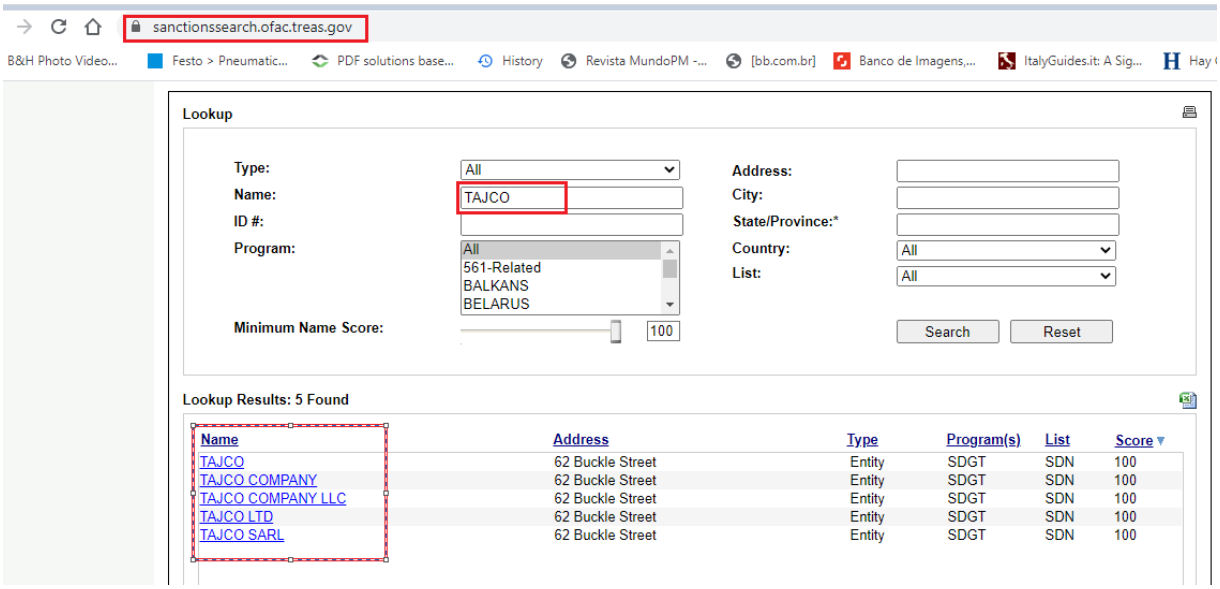
Por conta desta leis e regulamento o HSBC, assim como qualquer outro banco com operação naquele país, precisava verificar suas operações financeiras e reparar os problemas que foram apontados pelo OCC, o qual indicava que o sistema de monitoramento do banco como fraco e precisava ser reforçado, e foi para cumprir essas exigência que em 2010 um escritório em Delaware foi criado pelo HSBC.

Para esse escritório o HSBC contratou vários executivos e vários consultores, entre eles Everett Stern, executivo do banco que atuou como compliance officer do HSBC entre os anos de 2010 a 2011.

O trabalho de Stern, assim como de outras pessoas que foram trabalhar no mesmo escritório era 'limpar os alertas' gerados pelo sistema do banco. Os sistemas do banco estavam parametrizados conforme as diretrizes da OFARC e qualquer operação que fosse incompatível com essas regras, geravam alertas.

Por exemplo, se consultarmos a empresa "TAJCO[24]" na lista de pessoas com impedimento de realizar operação financeira com os Estados Unidos da América, encontraremos[25]:

22 Disponível em: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information acesso em 11/12/2020.
23 Disponível em: https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-data-files acesso em 12/12/2020.
24 Exemplo utilizado pelo Compliance Officer do HSBC na série da Netflix para explicar como o fator humano interfere na segurança da informação.
25 Lista de consulta pública disponível em: https://sanctionssearch.ofac.treas.gov/ acesso em 20/01/2020.



No *print* acima, destacado em vermelho, é possível verificar que na lista da OFARC aparecem todos as empresas com o nome 'TAJCO' que possuem restrições de realizar operações financeiras através dos sistema bancário norte-americano.

Assim, sempre que houver uma operação qualquer, envolvendo uma das empresas que esteja na lista de restrições, o sistema gera um alerta. O HSBC tinha um acúmulo muito grande destes alertas e este foi o motivador da estruturação do escritório em Delaware, era preciso "limpar" os alertas gerados, mas isso não queria dizer que o banco está agindo certo, mas ao menos estavam tentando agir corretamente.

O depoimento de Stern à *Netflix* indica que as pessoas que ali estavam a trabalhar não se mostravam interessadas a fazer o certo, estavam fazendo um trabalho sem realmente entender o que faziam. Stern descobriu várias transações realizadas as empresas que estavam na lista de restrições da OFARC e que haviam sido aprovadas pelo HSBC, o que estava errado. Ainda, Stern afirmou que o seu propósito de vida é "fazer o bem" indicando que queria "ter uma vida com um propósito e servir meu país e ser um instrumento para o bem e ser capaz de servir a um propósito maior" e assim três semanas após iniciar seu trabalho como executivo do HSBC começou a reportar as irregularidades à CIA (*Central Intelligence Agency of USA*).

O que Stern detectou como irregular nas operações realizadas no HSBC é que empresas, sancionadas ou banidas de realizarem operações financeiras com os EUA pela OFARC poderiam estar utilizando as fragilidades do sistema bancário para enviar dinheiro, por exemplo, a empresa 'TAJCO' que por sua vez poderia estar enviando dinheiro para o Hezbollah ou para Al Queda ou qualquer outra organização criminosa que estivesse listada pela OFARC.

A pergunta é como isso poderia acontecer se os sistemas do HSBC estavam parametrizados conforme as normas da OFARC? O que acontecia, segundo Stern, era que funcionários do HSBC faziam alterações dos nomes das empresas sancionadas ou banidas pela OFARC para manipular os sistemas do banco e possibilitar a remessa ilegal de dinheiro para terroristas e carteis de drogas.

Assim o que acontecia de forma mais específica, era que as operações que deveriam ser direcionadas a empresa "TAJCO" (nome que constava no sistema de restrições do banco) e assim seriam operações automaticamente negadas pelo sistema do banco, passam por manipulação humana e os nomes das empresas que apresentavam alguma restrição pela OFARC tinham seus nomes alterados de forma a burlar o sistema para por exemplo: "TAJ.CO" ou "T.A.J.C.O" ou ainda "TAJ/CO" e assim o sistema não detectava a irregularidade ou ainda quando detectava e gerava o alerta que eram tratados, também segundo Stern, por funcionários não comprometidos com suas atividades ou que não sabiam exatamente o que estavam a fazer.

Assim, com os reportes de Stern à CIA, iniciou-se uma investigação sobre os fatos que posteriormente levou o senado norte-americano a criar uma subcomissão para avaliar a conduta do HSBC, alegando que o banco estava usando suas filiais do México para lavar dinheiro, e fornecer dólares e acesso ao sistema financeiro dos EUA aos dos carteis de drogas, terrorismos. As investigações se forcaram nas negligencias do HSBC entre os anos de 2006 e 2009.

Em dezembro de 2012 o Banco HSBC fez um acordo com as autoridades norte-americanas que resultou no pagamento de valores da ordem de aproximadamente dois mil milhões de dólares. Ainda fazia parte do acordo a elaboração de uma carta de confissão pelos erros do banco e pela fraca gestão do monitoramento das suas operações e por último firmaram um compromisso público de reforçar o sistema de alertas e de

investigações internas, não podendo o HSBC (headquarter ou qualquer uma de suas filiais) pelos próximos 5 anos (2012 a 2017) incorrer em novas fraudes sob pena de perder a licença bancária de atuar como instituição financeira nos Estados Unidos[26].

4. O fator Humano na Segurança da Informação nas Organizações

Analisando os fatos acima é possível concluir que, no caso que envolveu o HSBC, não faria diferença quantos mil milhões de dólares o HSBC investiu em sistemas de segurança para fortalecer e garantir a legalidade das suas operações, a fraude continuaria a acontecer, pois o fator humano era a principal falha de toda a sua operação. Na lição de Kevin Mitnick:

> "*Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável*"[27].

A vulnerabilidade do fator humano nas organizações pode acontecer de várias maneiras, isso porque as motivações do ser humano, as emoções de cada um são muito variáveis e difíceis de prever, monitora ou evitar:

> "*O maior problema na segurança são as pessoas, que pelas suas características psicoemocionais podem facilmente serem manipuladas, induzidas, coagidas, ou forçadas a violar aspecto de segurança para conceder acesso ou privilégios a alguém, daí que, a*

26 Disponível em: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations acesso em 07/01/2021.
27 Ob. Cit. TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág. 03. In Mitnick & Simon (2002), p.15. – (Mitnick, K.& Simon, W.(2002). The art of deception: Controlling the human element of security. New York. John Wiley & Sons).

maior protecção contra a Engenharia Social, continua a ser a educação e consciencialização"[28].

As informações confidências de uma empresa, incluindo aqui as possíveis falhas de sistemas operacionais, podem ser obtidas de várias maneiras, como a manipulação psicológica de funcionários[29], coação, ameaças que posteriormente servirão para concretização da fraude.

No caso em tela, podemos verificar o fator humano atuando tanto no aspecto negativo, quanto no positivo:

O sentido negativo da atuação humana no caso do HSBC pode ser destacado na atuação humana que permitiu a execução da fraude interna, tendo em vista o conhecimento que se tinha sobre as falhas no sistema e de como burlá-las. O documentário da Netflix menciona, mas não há evidências que possam confirmar tal alegação no sentido de que muitos funcionários do Banco Bital eram corruptos e com a aquisição pelo HSBC esses funcionários corruptos agora tinham acesso ao sistema financeiro de um banco mundial, o que possibilitava a remessa de dinheiro ilegal para qualquer lugar do mundo. Ainda, também há indicação de que os cartéis de drogas do México usavam de coações físicas e morais, bem como valiam-se de ameaças constantes aos funcionários do Bital/HSBC, sinalizando que a sua integridade física e de suas famílias estariam comprometidas se não tivessem o apoio necessário para a realização das transações financeiras fraudulentas ou ilegais.

Soma-se a isso, ainda dentro do fator humano nas organizações, por afirmação do ex- executivo do HSBC (Stern) muitos funcionários do escritório do HSBC em Delaware, que foram contratados para "limpar" os alerta gerados pelos sistemas de detecção de fraude do banco, não estavam cientes da importância das suas atividades ou simplesmente não sabiam o que estavam a fazer.

Mas, ainda analisando o mesmo caso do banco HSBC (acusado de fraude contra o sistema financeiro, que pagou uma multa de quase dois mil milhões de dólares, e que também confessou a pratica de algumas práticas ilegais), há também o fator humano no

28 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 22.
29 Idem pág. 67.

seu aspecto positivo, que pode ser creditado a atitude, e ao olhar atento do ex-excutivo do banco que tinha como lema de vida “fazer o bem”, ou seja, a motivação deste colaborador era fazer a coisa certa, e assim conseguiu, com ajuda da CIA, dos procuradores gerais e demais autoridades envolvidas nas investigações, descobrir, interromper e corrigir uma falha interna do sistema bancário do banco HSBC.

5. Considerações Finais

Assim, após a análise do presente caso, que envolveu o banco HSBC México, com foco na contribuição humana tanto para a concretização da fraude, quanto para a resolução do problema, podemos afirmar que a segurança da informação nas organizações tem grande relação com pessoas: fator humano. Ainda que seja possível verificar que a maioria das empresas direcionam maior importância aos processos, software ou tecnologia para manter a segurança das informações, visto que os maiores investimentos são destinados a essas frentes.

A questão que poderia ser colocada aqui é: Para evitar fraudes internas, como a que aconteceu com o HSBC após a aquisição do Banco Bital, é necessário reduzir a interação do ser humano com processos relativos à segurança da informação? Nesse sentido, merece um alerta sobre este tema para que as empresas direcionem esforços (de tempo, de investimento, de capacitação) as questões relativamente aos processos de segurança da informação que envolvam pessoas, o que pode ser feito, por exemplo, estabelecendo políticas, normas e procedimentos de segurança da informação, bem como treinamentos de seus colaboradores de acordo com o nível académico e de atuação profissional de cada um.

É indispensável que as empresas conheçam suas vulnerabilidades e que proponham práticas para diminuir, atenuar ou reduzir riscos de exposição de seus negócios. Importante dizer que tudo isso é uma construção cultural que as empresas consolidam ao longo da sua existência focando sempre em boas práticas.

Por fim, gostaria de destacar a minha atuação profissional no HSBC Brasil, que se deu entre os anos de 2014 e 2016[30] como suporte consultivo criminal no departamento jurídico. A minha principal função era auxiliar as investigações internas com foco na prevenção a fraudes, bem como reportar as autoridades brasileiras qualquer irregularidade detectada fossem elas oriundas de fraude interna (provada por colaboradores) ou externas (clientes, hackers, estelionatos, etc.) sem qualquer filtro

30 Em 2016 o HSBC Bank Brasil S.A. – Banco Múltiplo foi adquirido pelo Banco Bradesco S.A. e deixou de ter atuação no mercado varejista brasileiro.

relativo a cargos, funções ou valores. Ainda, apenas a título ilustrativo naquela oportunidade seguíamos padrões rígidos de treinamentos relacionados as políticas de segurança da informação, prevenção a corrupção, suborno e lavagem de dinheiro, bem como sobre regras de monitoramento de fraudes internas.

6. Referência Bibliográficas

TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Disponível em: https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves

CORTEZ, Igor Siqueira e KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. 2021. Disponível em: https://www.researchgate.net/profile/Luis_Kubota/publication/259360942_Contramedidas_em_seguranca_da_informacao_e_vulnerabilidade_cibernetica_evidencia_empirica_de_empresas_brasileiras/links/00b7d52b31b2030da9000000/Contramedidas-em-seguranca-da-informacao-e-vulnerabilidade-cibernetica-evidencia-empirica-de-empresas-brasileiras.pdf.

MILLER, Andrew. Phishing: An Insidious Threat to Financial Institutions. 2006. https://www.bankinfosecurity.com/phishing-insidious-threat-to-financial-institutions-a-121

SILVA, Thiago Domingos de Souza. Segurança na Internet: Qual a nossa Vulnerabilidade? Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2603/2551

Sites

- https://comum.rcaap.pt/bitstream/10400.26/15403/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf
- https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves
- https://www.correiocidadania.com.br/colunistas/consciencia-negra/33-artigos/noticias-em-destaque?start=924
- https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations

- https://www.social-engineer.org/about/
- https://www.nytimes.com/2002/08/22/business/hsbc-buying-fifth-largest-bank-in-mexico-for-1.1-billion.html
- https://www.occ.treas.gov/
- https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
- https://sanctionssearch.ofac.treas.gov/
- https://www.27001.pt/iso27001_2.html
- https://www.techrepublic.com/blog/it-security/the-cia-triad/
- https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao

O IMPACTO DA CONSCIENCIALIZAÇÃO DOS COLABORADORES NA SEGURANÇA DA INFORMAÇÃO DAS ORGANIZAÇÕES

PEDRO LUCAS FARINHA*

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestrando em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

Nos últimos 10 anos, tem-se verificado um aumento progressivo no número de organizações que recorrem à utilização das tecnologias de informação e comunicação para desempenho das suas atividades. Em 2020, notou-se um impulso na adoção destas, por forma a garantir que várias organizações pudessem dar continuidade às suas atividades na crise pandémica que se instalou. No entanto, a utilização de novos métodos e tecnologias de trabalho levou a um acréscimo no número de ataques às organizações, aproveitando a falta de preparação destas e dos respetivos colaboradores para o novo contexto de trabalho.

Neste artigo, pretende-se avaliar a importância da consciencialização e educação dos colaboradores das organizações para a prevenção de ataques informáticos. Para tal, serão analisados três casos onde existiu negligência humana tanto nos comportamentos próprios para prevenção dos ataques, como na configuração de infraestruturas e funcionalidades tecnológicas. Estes serão utilizados para fundamentar a importância que a formação ou educação dos colaboradores das organizações em questão poderia ter tido na consciencialização dos mesmos na prevenção ou mitigação dos efeitos dos ataques.

Palavras-Chave: ataques; consciencialização, educação, e treino dos colaboradores; *hacking*, intrusões e phishing nas organizações; negligência; riscos.

ABSTRACT

In the last 10 years, there has been a progressive increase in the number of organizations who resort to the use of information and communication technologies to carry out their activities. In 2020, there was a strong impetus in its adoption, in order to ensure that several organizations could continue their activities in the pandemic crisis that was installed. However, the use of new methods and technologies of work has led to the addition of cyberattacks to organizations, taking advantage of the lack of preparation of these and their respective workers in this new context.

In this article, we intend to evaluate the importance of awareness and education of employees in the prevention of computer attacks. To this end, three cases of human negligence will be analyzed, both in terms of appropriate behaviors to the prevention, as well as in the configuration of infrastructures and technological functionalities. These will be used to substantiate the importance of training and educating employees and the importance of this in raising awareness on preventing or mitigating the effects of cyberattacks.

Keywords: ciberattacks; workers awareness, education, and training; hacking, intrusions and phishing in organizations; negligence; risks.

1. Introdução

De acordo com dados da OCDE [1], tem ocorrido um aumento progressivo nos últimos 10 anos no número de organizações que utilizam ou até dependem de Tecnologias de Informação e Comunicação (TIC) para desempenhar as suas atividades, o que evidencia a importância crescente destas no quotidiano empresarial.

Em 2020, a pandemia Covid19 levou a que inúmeras organizações tivessem como única possibilidade de trabalho, em regime não presencial, e de comércio, através de canais à distância (*e-commerce*). Tal fez com que houvesse um impulso substancial na adoção das TIC, e originou uma ainda maior dependência das organizações nestas, por forma a poderem assegurar a continuidade do negócio [2].

Em contrapartida, a adoção urgente de novas tecnologias e metodologias de trabalho obrigou a reorganizações consideráveis no funcionamento interno das organizações, muitas vezes sem que para tal existisse preparação prévia a nível tecnológico, ou consciencialização dos colaboradores para os riscos de segurança inerentes à introdução das novas condições.

Para além disso, as medidas introduzidas para a prevenção da pandemia originaram novas oportunidades de ataque. Em março de 2020, o Centro Nacional de Cibersegurança de Portugal registou um aumento de 176% no número de incidentes em comparação com o ano anterior, e um aumento de 217% no que toca à utilização de técnicas de *phishing*. Registou-se também a disponibilização na *darkweb*, de "*kits*", especialmente concebidos para a realização de ataques a indivíduos em teletrabalho, para além do aparecimento de aplicações *malware* e *ransomware*, dissimuladas com funcionalidades relacionadas com a pandemia Covid19 [3].

De acordo com a mesma entidade, não existe em Portugal uma generalidade de comportamentos e atitudes comparáveis à média da União Europeia no que toca à prevenção de vários riscos, apesar da consciencialização da existência de riscos como *phishing* e software malicioso. Não obstante, tem se verificado nos últimos anos uma

evolução positiva neste campo [4].

Kevin Mitnick defende na sua obra de 2003, "*The Art of Deception*", que apesar dos avanços e medidas de proteção trazidos pela componente tecnológica, apenas a combinação entre este fator e o humano poderão determinar o sucesso da manutenção da segurança da informação. Para tal, será necessário assegurar que todos os elementos que compõem a organização são consciencializados e devidamente treinados para reagir aquando da eminência de um ataque [5].

Nesta sequência, este artigo tem como objetivo evidenciar a importância que a formação e a consciencialização dos colaboradores têm, por forma a garantir segurança na informação das organizações.

Esta investigação abordará a técnica de "*phishing*", e a análise a um ataque deste tipo realizado a entidades públicas. De seguida, serão apresentadas algumas estratégias de mitigação para este tipo de ataque.

No que toca à componente tecnológica, será discutido o conceito de vulnerabilidade e falha tecnológica, e será apresentado um caso em que a manutenção desta componente foi descorada pela parte humana bem como houve negligência das próprias equipas técnicas de uma organização.

2. Ataques ao Fator Humano

*"**Phishing**"* é uma técnica de engenharia social, utilizada por atacantes, com o objetivo de coagir as vítimas a fornecer informações privilegiadas, tais como credenciais ou números de cartões de crédito, ou a realizar ações fraudulentas, sem que de tal se apercebam. Este tipo de ataque é habitualmente levado a cabo através do envio massivo de mensagens de email, as quais aparentam ser provenientes de entidades fidedignas e relevantes, como departamentos governamentais ou instituições bancárias [6].

Não obstante, a atividade de *phishing* pode ser realizada com recurso a outros meios de contacto, como chamadas telefónicas ou mensagens SMS.

De acordo com a *Proofpoint* [7], 99% dos ataques de email maliciosos requer interação humana, vulgo "ajuda" do utilizador para levar a cabo o seu objetivo. Tal pode consistir na abertura de um documento anexado à mensagem, de um endereço de internet, ou na aceitação de um aviso de segurança que fora despoletado na sequência da deteção de uma possível fraude. Poderá, também, consistir na simples resposta à mensagem com a informação requisitada.

As origens do "*phishing*" remontam a meados de 1990, em que grupos de adolescentes procuravam obter acesso gratuito ilegítimo ao provedor de acesso Internet AOL, na altura suportado por ligações telefónicas [8]. Para tal, foi desenvolvido um software que automatizava o envio de mensagens fraudulentas para clientes do fornecedor, enquanto estes frequentavam as salas de *chat* deste [Figura 1].

Figura 1 - Programa de envio automático de mensagens fraudulentas

Nestas, os atacantes identificavam-se como colaboradores da empresa, solicitando aos clientes a atualização de dados pessoais, como as respetivas palavras-passe de acesso e/ou os números de cartões de crédito.

Este tipo de ataque era possível em parte devido à arquitetura tecnológica utilizada na altura. Em primeiro lugar, apesar do serviço funcionar sobre a infraestrutura da rede telefónica pública, a operadora que o suportava não disponibilizava ou mantinha registos dos números de onde as chamadas originavam.

Assim, a impossibilidade de identificar a origem dos ataques, permitia aos agentes maliciosos um acesso anónimo ao serviço, sem que estes corressem o risco de ser identificados e responsabilizados.

Por outro lado, o fornecedor do acesso Internet não realizava validações de cartões de crédito em tempo real, o que por si só, já permitia aos atacantes obter acesso temporário ao serviço, o qual poderia ser utilizado para levar a cabo os ataques.

Tal perdurou até 1995, altura em que o operador implementou medidas de validação de cartões.

No decorrer dos anos, o *phishing* sofreu várias evoluções. Uma variante deste tipo de ataque denomina-se de *spear phishing*, no qual é realizado um ataque dirigido a uma pessoa, um grupo de pessoas em particular, ou a uma organização específica. Para tal, é necessário que seja realizada uma investigação prévia da vítima, por forma a gerar mensagens com maior credibilidade.

Estes tipos de ataque podem ter o seu risco de sucesso reduzido através da sensibilização dos colaboradores para pequenos detalhes nas mensagens de email, tais como erros ortográficos, linguagem inadequada ao tipo de pedido (como a formalidade), ou na análise crítica da probabilidade de certos pedidos serem dirigidos à pessoa em questão. Adicionalmente, a utilização da autenticação multifator reduz a probabilidade de sucesso não só deste, mas ataques que envolvam o comprometimento de credenciais.

Um caso de *spear phishing* realizado com sucesso, é o da captura de credenciais da

conta de John Podesta, na altura, gestor da campanha de candidatura à presidência dos Estados Unidos de Hillary Clinton [9].

De acordo com a CBS News, Podesta recebeu na sua caixa de correio, um alerta relativo a um acesso ilegítimo à sua conta, proveniente de um país estrangeiro, o qual incluía um *link*, através do qual a palavra-passe poderia ser reposta.

Por precaução, o gestor de campanha consultou o suporte IT, através da sua assistente, que reencaminhou o email original para os técnicos. Estes, afirmando a legitimidade da mensagem, sugeriram não só a reposição da palavra-passe, mas também a ativação da autenticação multifator, tendo para tal, disponibilizado um link adequado para o efeito.

Apesar disso, os técnicos de suporte não verificaram que o próprio *link* no email recebido originalmente, remetia para um abreviador de endereços ("*bit.ly*"), que não pertencia ao fornecedor de serviços de e-mail [Figura 2].

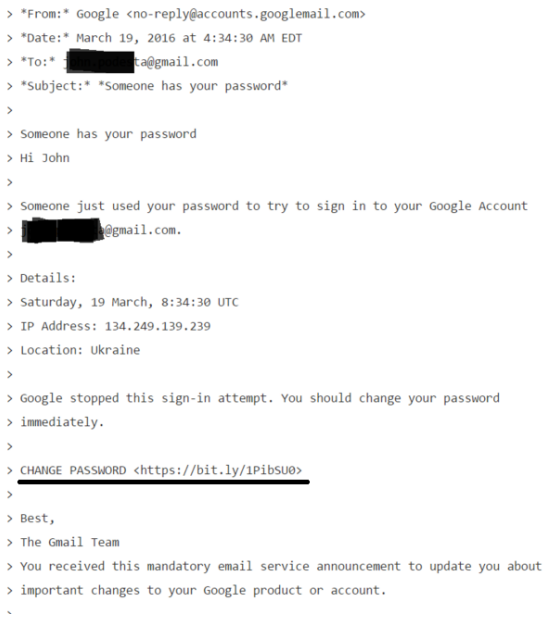

> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Figura 2 - Email fraudulento recebido por John Podesta

Na sequência da troca de mensagens, a vítima utilizou o *link* disponibilizado pelo atacante, e não o sugerido pelo técnico de suporte, levando a que as suas credenciais

fossem comprometidas. Esta ação deu ao atacante acesso à caixa de correio da vítima, tendo o respetivo conteúdo sido alegadamente divulgado no site *Wikileaks* [10].

Neste caso, é evidente a falha da componente humana.

Por um lado, a negligência por parte dos intervenientes ditou o comprometimento do acesso. O cuidado da vítima em confirmar com o técnico de IT a legitimidade do email, não fora suficiente para prevenir o ataque, uma vez que este último não alertou a vítima do *link* fraudulento.

Neste caso, tanto o gestor da campanha, como a própria candidata optaram por utilizar endereços de email pessoais ao invés de corporativos, por forma a tentar evitar possíveis escrutínios ou a divulgação de conteúdos inadequados [11].

Por outro lado, a utilização de um serviço de email pessoal não permitiu à equipa de IT ter a capacidade de impor políticas de segurança adequadas à natureza da informação, tais como a deteção automatizada de fraudes, a obrigação da rotação periódica de *passwords* e a ativação da autenticação multifator, conforme sugerido pelo técnico. Adicionalmente, com a utilização deste tipo de serviço, não foi possível à equipa de IT monitorizar proactivamente os acessos às contas.

Estas medidas, em particular a autenticação multifator, poderiam ter mitigado ou evitado o sucesso do ataque, dado que mesmo conhecendo as credenciais (utilizador e palavra-passe), o atacante estaria obrigado a apresentar um segundo fator de autenticação, como palavras-passe de utilização única, cujo gerador estaria, idealmente, na posse do titular legítimo da conta [11] [12].

Neste ataque, apesar de terem ocorrido quebras na segurança, não foram exploradas quaisquer vulnerabilidades tecnológicas, mas sim, vulnerabilidades *humanas* e na configuração tecnológica realizada pelos intervenientes [12].

Outro exemplo em que a correta adoção de medidas tecnológicas poderia ter mitigado, ou evitado o sucesso do ataque, foi em 2017, em que a página de uma rede social da empresa de Cibersegurança *McAfee* foi alvo de *defacing*.

Nesta situação, um dos ex-gestores mantinha acesso de administração à página,

mesmo quando já não tinha responsabilidades para com a empresa. De acordo com a investigação realizada, as credenciais do ex-colaborador foram comprometidas num ataque que levou à divulgação de credenciais de utilizadores de uma outra rede social.

A investigação concluiu que o ex-colaborador utilizou a mesma palavra-passe para todas os seus perfis, e procedeu à alteração da mesma, na rede que sofreu o ataque, e não na rede onde lhe tinham dado acessos de gestão à página da *McAfee*.

Tanto o ex-colaborador como a própria empresa de cibersegurança apresentaram falhas. O primeiro, por ter adotado a reutilização de palavras-passe, e não ter utilizado mecanismos que pudessem ajudar a melhorar a segurança das suas contas, como é o caso da autenticação multifator. A empresa, no entanto, deveria ter revogado os privilégios do ex-colaborador quando estes deixaram de fazer sentido.

Este ataque levou a um dano de imagem à empresa, já que a própria empresa tinha como missão a proteção dos seus clientes de ataques deste tipo, e ela própria fora atacada [13][14].

Com base nestes exemplos, será incorreto assumir-se que a prevenção de ataques com origem humana será exclusiva das equipas de segurança informática. A consciencialização dos utilizadores e a responsabilidade destes por pequenos pormenores fará parte de um conjunto de medidas de elevada importância para assegurar a segurança das organizações.

3. Ataques Tecnológicos

Apesar do constante aumento de ataques de engenharia social ou de ataques baseados em erros humanos, o número de novas vulnerabilidades tecnológicas detetadas anualmente, tem também vindo a aumentar, sendo que nos últimos 4 anos, teve um aumento muito considerável face aos anos anteriores, conforme mostra o gráfico da Figura 3.

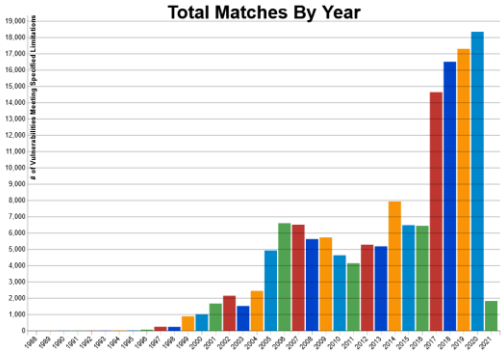


Figura 3 - Evolução do número anual de vulnerabilidades tecnológicas divulgadas pelo NIST [15]

A base de dados de CVE's (*Common Vulnerabilities and Exposures*) do *National Institute of Standards and Technology* (NIST National Vulnerabilities Database) é uma base de dados de vulnerabilidades conhecidas, mantida pelo governo dos Estados Unidos, na qual é feita a respetiva classificação, tendo em conta a natureza, severidade, e outros fatores relevantes para a sua indexação [15].

Acompanhando o número de vulnerabilidades detetadas, a proporção do número de vulnerabilidades com severidade "Média" e "Alta" tem também vindo a aumentar[1].

1 À data da escrita deste artigo, cerca de 2000 vulnerabilidades foram publicadas no ano de 2021. No entanto, a tendência para o aumento da percentagem de vulnerabilidades com maior severidade aparenta se manter, visto que em fevereiro, o número de vulnerabilidades com severidade "Média" ou "Alta" é já superior ao número de vulnerabilidades com severidade "Baixa".

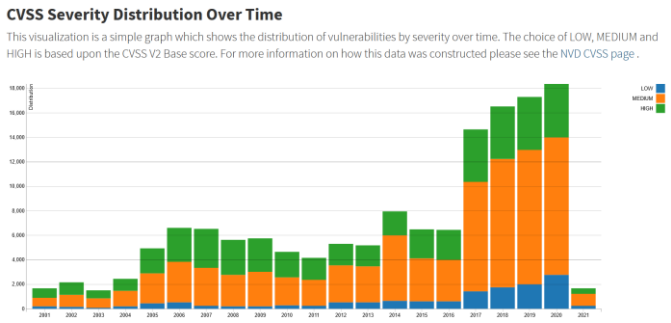


Figura 4 - Distribuição de severidade das vulnerabilidades ao longo do tempo [15]

A divulgação deste tipo de informação tem como objetivo lançar o alerta para a existência de possíveis riscos de ataque, tendo com intuito a promoção da necessidade da remediação destes.

No entanto, esta divulgação pública poderá também ser utilizada como um elemento guia para os atacantes, dado que nem sempre as organizações dão atenção proativa a este tipo de questões, como será discutido no caso abaixo analisado.

Em 2017, a agência de crédito *Equifax* foi alvo de um ataque de *hacking* à sua infraestrutura tecnológica, que levou à extorsão da informação pessoal e financeira de cerca de 140 milhões de cidadãos, a maioria de nacionalidade americana.

A 6 de março daquele ano, a *Apache Software Foundation* divulgou a vulnerabilidade CVE-2017-5638, a qual permitia a execução remota de código em aplicações web baseadas em determinadas versões da *framework Apache Struts* [16][17][18].

Esta falha, presente num sistema legado para gestão de disputas de clientes da *Equifax*, exposto à *Internet*, não tardou em ser explorada.

Pouco tempo depois da divulgação pública da falha, surgiram provas de conceito a demonstrar a sua exploração, cuja utilização foi identificada pela *Cisco Talos Intelligence Group*, em sistemas monitorizados por si [19].

Inicialmente, a exploração da falha foi utilizada para a execução de comandos simples, que permitiam a recolha de informações, como a identificação do utilizador com

o qual a aplicação executava, ou informações relativas aos sistemas remotos.

No entanto, houve uma rápida evolução para a execução de comandos mais complexos, tais como a desativação de *firewalls* e a descarga de código binário para execução remota, que levou à implementação de sistemas *webshell*, de forma a permitir aos atacantes outras formas de aceder aos sistemas sem recorrer à exploração da falha, caso esta fosse eventualmente corrigida [20][21].

De acordo com a agência de notícias *Bloomberg*, o ataque e intrusão à *Equifax* teve início 4 dias após a divulgação pública da falha, apesar do investimento considerável em medidas de proteção tecnológicas.

Ainda antes do ataque, uma consultora contratada para a avaliação de segurança da Equifax identificou várias falhas na configuração tecnológica dos sistemas, bem como na aplicação de correções para remediação de vulnerabilidades.

Adicionalmente, a saída e rotação de elementos-chave da empresa em anos anteriores, como o *Chief Information Security Officer*, contribuiu de forma negativa para a manutenção de políticas de segurança estáveis na *Equifax*. Por essa altura, era opinião comum de vários elementos que a segurança era descorada, a favor da entrega de resultados [22].

Apesar dos alertas, a agência de crédito declinou corrigir ou assumir as falhas, argumentando, com a opinião da investigação não ter sido levada a cabo por elementos com a senioridade adequada [23].

Quatro meses depois, em finais de julho de 2017, a equipa técnica da *Equifax* deu conta do ataque durante a realização de operações de rotina num equipamento de rede destinado à interceção e análise de tráfego encriptado.

Aquando da renovação de um certificado digital expirado, um membro da equipa de comunicações identificou padrões de tráfego fora do comum, nos quais verificou a execução de comandos fora dos parâmetros e métodos habituais, pelo que procedeu de imediato ao bloqueio das origens de tráfego, e ao reporte do caso a níveis superiores, o que levou a *Equifax* a despoletar o início da investigação, recorrendo à consultora anteriormente contratada.

Foi concluído que o certificado em questão esteve em uso durante cerca de 10 meses depois de ter expirado. Desta forma, não foi possível detetar a intrusão, uma vez que não era possível ao equipamento de rede desencriptar o tráfego encriptado [24].

Apesar de também não existir preservação de registos (*logs*[2]) a longo prazo, a análise forense permitiu aos auditores reconstruir em detalhe as ações levadas a cabo pelos atacantes, que serviram de *input* para as investigações levadas a cabo.

Entre elas, o Comité de Investigação do Senado dos Estados Unidos considera que houve negligência na forma como a agência zelava pela segurança do seu parque informático.

Em 2015 foi implementada uma política de segurança para gestão de vulnerabilidades e implementação de correções, a qual identificou mais de 8500 vulnerabilidades, nas quais um número acima de 1000 era considerado de severidade "Média" ou "Alta". Até então, a *Equifax* não detinha qualquer política formal para implementação de correções na companhia.

No entanto, não foi dado seguimento formal para a execução da política, pelo que a agência optou por seguir uma abordagem reativa, em que apenas aplicaria correções, caso os sistemas de *scanning* as identificassem, o que neste caso, não aconteceu.

Ainda que a vulnerabilidade utilizada para o ataque tivesse sido discutida em reuniões mensais, a respetiva correção não foi implementada imediatamente, em parte devido à complexidade dos procedimentos impostos, que obrigava a um envolvimento de várias entidades da organização por forma a coordenar a atividade de *patching*.

A não atualização do sistema de inventariação fez também com que a própria existência do componente com a vulnerabilidade não fosse considerada. Outro fator causado pela não implementação da correção está também relacionado com o alerta para a existência da vulnerabilidade não ter sido comunicado ao responsável pelo sistema afetado.

O Comité de Investigação defende também que houve negligência na gestão da

2 "*Logs*" são registos de atividade de sistemas informáticos, úteis para recriar os passos executados por atacantes.

infraestrutura. A expiração de um certificado digital fez com que deixasse de existir monitorização de tráfego encriptado, o que só foi remediado durante uma operação de rotina, tendo sido ignorado um alerta gerado pela monitorização. [20] [23].

A nível de arquitetura técnica, o impacto do ataque poderia ter sido igualmente reduzido caso tivesse sido adotada uma segmentação a nível de rede. Não havendo segmentação, o acesso a uma base de dados permitiu aceder a várias outras, incluindo a um repositório onde se encontravam credenciais não encriptadas para outras bases de dados.

Esta decisão de arquitetura foi tomada com o intuito de favorecer a usabilidade e aumentar a eficiência na implementação de operações do negócio, no entanto, comprometendo e descorando a segurança e indicações do NIST.

Em comparação, o Comité refere duas outras entidades concorrentes que detinham serviços afetos pela vulnerabilidade.

Nestas, a definição e imposição formal de políticas de segurança, prazos e procedimentos para aplicação de correções, a realização de análises periódicas aos elementos inventariados, os quais eram mantidos atualizados, permitiram à *Experian* e à *TransUnion* proceder à aplicação proativa das correções necessárias, não havendo registos de acessos indevidos com recurso à vulnerabilidade que afetou a *Equifax* [25].

David Webb, na altura *Chief Information Officer* da *Equifax*, assume que o ataque poderia ter sido evitado, caso a vulnerabilidade que motivou o ataque tivesse sido corrigida.

Não obstante, não são claras as razões que levaram a *Equifax* a ignorar recomendações do NIST, ou os requisitos de segurança das suas próprias políticas [20] [25]. Como consequência, a agência viu várias das suas certificações como a ISO 27001 e *Payment Card Industry* (PCI) suspensas, na sequência do ataque [26].

4. A eficácia da Formação

Um estudo realizado em 2009 numa organização ligada ao ramo do transporte de mercadorias da República da Turquia sobre a formação na segurança de informação nas organizações, revela que grande parte dos incidentes se devem a erros não intencionais, e ao desconhecimento de boas práticas de segurança e tecnológicas por parte dos colaboradores, tais como a utilização de *palavras-passe* de fácil adivinhação, abandono de equipamentos informáticos sem os proteger, entre outras [27].

Neste estudo, foram levadas a cabo várias sessões de formação, por forma a contribuir para a elucidação dos colaboradores sobre bons costumes que possam ajudar a prevenir quebras na segurança.

Para avaliar a eficácia da formação dos utilizadores, foram realizadas várias auditorias de segurança à complexidade das palavras-passe, bem como definidos patamares de objetivos que deveriam ser cumpridos ao fim de um determinado prazo.

A consciencialização dos colaboradores da organização para a necessidade da utilização de palavras-passe com alta complexidade teve efeitos positivos. Um universo de cerca de 3000 utilizadores, teve as respetivas palavras-passe sujeitas a ataques de força bruta durante 24 horas, sendo que o número de palavras-passe que resistiu aos mesmos, passou de 1,2% para 36,4% no espaço de um ano.

Um outro estudo realizado em 2019 [28], avalia a preferência de utilizadores sobre os métodos utilizados para a formação, e a respetiva eficiência na resposta a ataques de *phishing*.

Apesar do estudo não ter chegado a uma conclusão concreta no que toca à preferência do tipo de formação entre a leitura de documentação, a assistência a vídeos, formação presencial, ou recurso a jogos interativos educacionais, este chega a resultados positivos, em que os participantes do estudo demonstraram uma melhoria na identificação de ataques de *phishing* após qualquer uma das diferentes formações ministradas.

Tendo em conta os estudos e as recomendações supracitadas, verifica-se que a formação de *soft-skills* e de boas práticas tem um papel relevante na consciencialização dos utilizadores na segurança da informação das organizações, as quais, se aplicadas, poderiam ter evitado ou mitigado os ataques das entidades nos exemplos anteriores.

No que toca à educação tecnológica, as investigações concluem que a agência do exemplo exposto não mantinha práticas consistentes com as recomendações da *framework* de cibersegurança do NIST [29], nem as equipas técnicas estavam preparadas para aplicar as políticas em vigor.

Apesar de voluntária, a aplicação de várias recomendações da *framework* do NIST poderia ter mitigado, ou evitado o ataque, tal como confirmado pelo CIO David Webb.

Alguns exemplos de recomendações que não foram aplicadas:

- Não existia inventariação adequada que permitisse identificar a utilização de determinadas componentes de *software*, e onde as mesmas estavam implementadas (ID.AM-1/ID.AM-2);
- Não existia segregação ou segmentação de redes, de forma a isolar sistemas heterogéneos (PR.AC-5);
- Não existia documentação ou um processo proativo de mitigação de vulnerabilidades constantes nos componentes de *software* (RS.MI-3);
- A deteção de intrusão não se encontrava em funcionamento devido à não renovação proativa um certificado digital (DE.CM-1/DE.CM-4/DE.CM-7);
- Existiam credenciais armazenadas de forma desprotegida (PR.AC-4);
- Não existia uma política de retenção de *logs* adequada (PR.MA-2).

À semelhança das formações para preparação de *phishing*, a formação técnica e em segurança *poderia* ter alavancado a consciencialização das equipas técnicas para a importância do seguimento de boas práticas, e melhorar a dedicação destas no que toca à manutenção dos sistemas internos, por forma a prevenir ataques deste, e de outros tipos.

Os relatórios não referem a existência de formações lecionadas às equipas antes do incidente. É dada, no entanto uma recomendação de formação das equipas relativa aos procedimentos internos de segurança.

5. Conclusão

Esta investigação permitiu, em primeiro lugar, rever três fenómenos criminosos dos tempos atuais, cuja atuação tem vindo a comprometer de forma significativa a segurança da informação de inúmeras organizações nos últimos anos.

Seguindo a tendência atual, o desenvolvimento de novas soluções tecnológicas apresentará novas funcionalidades que poderão ser utilizadas para otimizar a produtividade empresarial, bem como o quotidiano da população em geral.

A adoção das novas tecnologias irá inevitavelmente introduzir novos vetores de ataque que serão alvo de exploração por agentes maliciosos, tendo em vista tanto a negligência individual, desconhecimento, ou vulnerabilidades das tecnologias envolvidas.

A análise do caso de *phishing* permitiu evidenciar a facilidade com que o elemento humano é passível de ser explorado. O caso exposto, em particular, demonstra como os próprios elementos de equipas de suporte tecnológico, e com formação para tal, não são suficientes para prevenir um ataque dirigido, caso não seja dado um especial cuidado aos detalhes do mesmo.

Por outro lado, a conduta da vítima, apesar de inicialmente prudente, provou também não ser suficiente, uma vez que as indicações dadas pelo especialista não foram seguidas em pormenor, apesar deste último não ter identificado o risco iminente.

O caso de *defacing* à empresa de cibersegurança, também relacionado com descuido humano, permitiu comprovar que nem sempre as organizações especializadas seguem à risca as políticas que elas próprias defendem, caso os seus colaboradores não as pratiquem, o que sugeriu o impacto na que tal pode causar na imagem da organização.

No que toca ao caso de *hacking*, verificou-se um conjunto de fatores que permitiram a intrusão e fuga de informação dos sistemas da agência de crédito.

A falta de acompanhamento e de seguimento das políticas de segurança definidas deu origem a entropia entre as várias equipas da organização, o que demonstra que a definição de uma política de segurança por si não foi suficiente para a garantir.

Por outro lado, notou-se negligência por parte das equipas técnicas na gestão da infraestrutura informática, apesar de tecnologicamente, os equipamentos e funcionalidades necessárias para garantir a segurança, estarem presentes.

A falta de manutenção do equipamento de análise de tráfego encriptado ou a opção pela não segmentação de redes foram elementos que poderiam ter diminuído o impacto do ataque.

A ausência de uma política eficiente de aplicação de correções, e consequente não aplicação da correção que possibilitou o ataque, foi, de acordo com o *CIO* da altura, um elemento que poderia ter evitado a intrusão, por completo.

Por fim, não são claras as razões que levaram a *Equifax* a ignorar vários procedimentos, tendo-se verificado uma desconsideração generalizada no que toca à importância segurança da organização.

Adicionalmente, os relatórios do caso não referem ter sido dado qualquer tipo de formação às equipas técnicas antes do incidente.

No entanto, verifica-se uma recomendação em formar as equipas para os procedimentos internos, uma vez que aparentemente vários destes não foram levados a cabo adequadamente, devido à complexidade como os mesmos deveriam ser aplicados, ou por mero desconhecimento das equipas.

Assume-se que a *Equifax* poderia ter beneficiado com a educação das equipas técnicas, por forma a formalizar não só os procedimentos a adotar para a manutenção dos sistemas de segurança, como por exemplo, a importância para a renovação proativa de certificados digitais, mas também a nível tecnológico, onde não só a segurança, com a manutenção em geral dos sistemas empresariais poderia beneficiar, como por exemplo, com a segmentação de redes [30].

"*A cibersegurança é um desporto coletivo, no qual todos têm de desempenhar o seu papel (…). As ferramentas podem ser de grande utilidade, mas apenas a conjugação de pessoas, ferramentas, [e] procedimentos (…) permite uma defesa eficiente*" [14].

Em suma, nota-se que em todos os exemplos apresentados, os incidentes apresentados recaem em pontos que não foram assegurados, nomeadamente na conjugação entre o fator humano com o tecnológico. Um não será suficiente sem o outro para garantir a segurança das organizações, nem tampouco será suficiente a uma equipa de segurança garantir que uma organização está segura, caso os seus utilizadores não sigam boas práticas.

REFERÊNCIAS

[1] OECD, «ICT Access and Usage by Businesses». 2021, [Em linha]. Disponível em: https://stats.oecd.org/.

[2] S. Fernandez, B. Vieira, P. Jenkins, e McKinsey, «Europe's migration to digital services during COVID-19 | McKinsey». https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages (acedido Jan. 31, 2021).

[3] Centro Nacional de Cib, «Relatório Riscos & Conflitos 2020», 2020.

[4] CNCS, «Relatório Cibersegurança em Portugal - Sociedade 2020», 2020.

[5] K. D. Mitnick e W. L. Simon, *The Art of Deception: Controlling the Human Element in Security*. 2002.

[6] «ENISA Threat Landscape 2020 - Phishing», 2020, [Em linha]. Disponível em: https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.

[7] Proofpoint, «Human Factor Report 2019», 2019, [Em linha]. Disponível em: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf.

[8] K. Rekouche, «Early Phishing», pp. 1–9, 2011, [Em linha]. Disponível em: http://arxiv.org/abs/1106.4692.

[9] K. Krawchenko, «The phishing email that hacked the account of John Podesta», *CBS Interactive Inc.*, 2016. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ (acedido Fev. 03, 2021).

[10] «WikiLeaks - The Podesta Emails». https://wikileaks.org/podesta-emails/ (acedido Fev. 04, 2021).

[11] R. Mitchell, «The Podesta Emails - Anatomy of an attack». https://p3isys.com/p3isys-tech-blog/153-podestahack (acedido Fev. 04, 2021).

[12] J. Koebler, «Basic Digital Security Could Have Prevented One of the Biggest Political Scandals in American History». https://www.vice.com/en/article/ywkd35/two-factor-authentication-russia-hacking-indictment (acedido Fev. 09, 2021).

[13] «McAfee LinkedIn page hijacked | CSO Online». https://www.csoonline.com/article/3190163/mcafee-linkedin-page-hijacked.html (acedido Fev. 06, 2021).

[14] A. Cerra, *The Cybersecurity Playbook*, 1st ed. Wiley, 2019.

[15] «NVD - Statistics». https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all (acedido Fev. 06, 2021).

[16] NIST.gov, «nvd - cve-2017-5638», *Nvd.nist.gov*. 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[17] «Apache Struts 2 Vulnerability Leads to RCE». https://www.trendmicro.com/en_us/research/17/c/cve-2017-5638-apache-struts-vulnerability-remote-code-execution.html (acedido Fev. 07, 2021).

[18] Lukasz Lenart, «S2-045 - Apache Struts 2 Wiki - Apache Software Foundation», 2016. https://cwiki.apache.org/confluence/display/WW/S2-045 (acedido Fev. 07, 2021).

[19] «GitHub - tengzhangchao/Struts2_045-Poc: Struts2-045 POC». https://github.com/tengzhangchao/Struts2_045-Poc (acedido Fev. 07, 2021).

[20] US HoR, «The Equifax Data Breach», *US House Represent. Comm. Overs. Gov. Reform*, vol. 87, n. 12, p. 14, 2018, [Em linha]. Disponível em: http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=126654696&site=eds-live&scope=site.

[1] OECD, «ICT Access and Usage by Businesses». 2021, [Em linha]. Disponível em: https://stats.oecd.org/.

[2] S. Fernandez, B. Vieira, P. Jenkins, e McKinsey, «Europe's migration to digital services during COVID-19 | McKinsey». https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages (acedido Jan. 31, 2021).

[3] Centro Nacional de Cib, «Relatório Riscos & Conflitos 2020», 2020.

[4] CNCS, «Relatório Cibersegurança em Portugal - Sociedade 2020», 2020.

[5] K. D. Mitnick e W. L. Simon, *The Art of Deception: Controlling the Human Element in Security*. 2002.

[6] «ENISA Threat Landscape 2020 - Phishing», 2020, [Em linha]. Disponível em: https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.

[7] Proofpoint, «Human Factor Report 2019», 2019, [Em linha]. Disponível em: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf.

[8] K. Rekouche, «Early Phishing», pp. 1–9, 2011, [Em linha]. Disponível em: http://arxiv.org/abs/1106.4692.

[9] K. Krawchenko, «The phishing email that hacked the account of John Podesta», *CBS Interactive Inc.*, 2016. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ (acedido Fev. 03, 2021).

[10] «WikiLeaks - The Podesta Emails». https://wikileaks.org/podesta-emails/ (acedido Fev. 04, 2021).

[11] R. Mitchell, «The Podesta Emails - Anatomy of an attack». https://p3isys.com/p3isys-tech-blog/153-podestahack (acedido Fev. 04, 2021).

[12] J. Koebler, «Basic Digital Security Could Have Prevented One of the Biggest Political Scandals in American History». https://www.vice.com/en/article/ywkd35/two-factor-authentication-russia-hacking-indictment (acedido Fev. 09, 2021).

[13] «McAfee LinkedIn page hijacked | CSO Online». https://www.csoonline.com/article/3190163/mcafee-linkedin-page-hijacked.html (acedido Fev. 06, 2021).

[14] A. Cerra, *The Cybersecurity Playbook*, 1st ed. Wiley, 2019.

[15] «NVD - Statistics». https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all (acedido Fev. 06, 2021).

[16] NIST.gov, «nvd - cve-2017-5638», *Nvd.nist.gov*. 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[17] «Apache Struts 2 Vulnerability Leads to RCE». https://www.trendmicro.com/en_us/research/17/c/cve-2017-5638-apache-struts-vulnerability-remote-code-execution.html (acedido Fev. 07, 2021).

[18] Lukasz Lenart, «S2-045 - Apache Struts 2 Wiki - Apache Software Foundation», 2016. https://cwiki.apache.org/confluence/display/WW/S2-045 (acedido Fev. 07, 2021).

[19] «GitHub - tengzhangchao/Struts2_045-Poc: Struts2-045 POC». https://github.com/tengzhangchao/Struts2_045-Poc (acedido Fev. 07, 2021).

[20] US HoR, «The Equifax Data Breach», *US House Represent. Comm. Overs. Gov. Reform*, vol. 87, n. 12, p. 14, 2018, [Em linha]. Disponível em: http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=126654696&site=eds-live&scope=site.

[21] «Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Content-Type: Malicious - New Apache Struts2 0-day Under Attack». https://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html (acedido Fev. 07, 2021).

[22] M. Riley, J. Robertson, e A. Sharpe, «The Equifax Hack Has the Hallmarks of State-Sponsored Pros - Bloomberg», *Bloom. Technol.*, pp. 1–6, 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em:

https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

[23] J. Fruhlinger, «Equifax data breach FAQ: What happened, who was affected, what was the impact?», *CSO*, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (acedido Fev. 02, 2021).

[24] «New evidence raises doubts about executives' handling of the Equifax breach - The Verge». https://www.theverge.com/2017/9/19/16332096/new-evidence-raises-doubts-about-executives-handling-equifax-breach (acedido Fev. 07, 2021).

[25] Permanent Subcommittee on Investigations e United States Senate, «How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach», 2019.

[26] Equifax Inc., «2018 Annual Report», 2018. Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual Reports/2018-annual-report.pdf.

[27] M. Eminağaoğlu, E. Uçar, e Ş. Eren, «The positive outcomes of information security awareness training in companies - A case study», *Inf. Secur. Tech. Rep.*, vol. 14, n. 4, pp. 223–229, Nov. 2009, doi: 10.1016/j.istr.2010.05.002.

[28] K. F. Tschakert e S. Ngamsuriyaroj, «Effectiveness of and user preferences for security awareness training methodologies», *Heliyon*, vol. 5, n. 6, p. e02010, 2019, doi: 10.1016/j.heliyon.2019.e02010.

[29] «Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1», Gaithersburg, MD, Abr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[30] S. Laan, *IT Infrastructure Architecture-Infrastructure Building Blocks and Concepts Third Edition*. Lulu. com, 2017.

A SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES NO *NOVO NORMAL* (COVID-19)

RUI FILIPE BARATA PEREIRA*

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestrando em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

A Segurança da Informação em geral e nas Organizações em particular é um tema de importância crescente, contínua e consistentemente, nestas últimas décadas. É um elemento e uma preocupação presente no dia a dia das mais variadas atividades, seja na esfera da área pessoal, individual e social, seja nos serviços e organizações públicas como saúde, justiça, segurança e governação em geral, seja nos serviços e organizações privadas tanto nos sectores primário como secundário e terciário. Por isto tudo é também afetado por uma grande diversidade de eventos e transformações que vão surgindo nas sociedades modernas. Assim eventos como esta mais recente realidade provocada pela Pandemia do Covid-19 têm um impacto muito significativo na abordagem do tema da Segurança da Informação e em especial no que se refere ao tema de estudo deste trabalho, a segurança da informação nas organizações no novo normal (Covid-19).

Palavras-Chave: Segurança da Informação; Segurança da Informação nas Organizações; Pandemia e COVID-19; Cibersegurança.

ABSTRACT

Information Security in general and in Organizations is a topic of increasing and continuous importance in these last decades. Be it in the sphere of personal, individual and social areas, or in public services and organizations such as health, justice, security and government in general, or in services and private organizations either in the primary, secondary and/or tertiary sectors, is a factor as well as a concern supported in the day to day of these varied activities. In addition to all this, it is still affected by a great diversity of events and transformations that are emerging in modern societies. Thus, events like this most recent reality caused by the Covid-19 Pandemic have a very significant impact in addressing the topic of Information Security and regarding this work, namely, information security in organizations in the *new normal* (Covid-19).

Keywords: Information security; Information Security in Organizations; Pandemic and COVID-19; Cybersecurity.

1. Introdução

Este trabalho foca-se no caso das organizações em que a sua área de negócio permite o trabalho remoto, nomeadamente a Indústria de serviços.

O impacto da Pandemia Covid-19, no que concerne a este tema de estudo, levou a que as Organizações fossem obrigadas a uma drástica mudança para um ambiente de trabalho remoto.

Esta alteração dos modos de trabalho forçou uma acelerada Transformação Digital nas Organizações. Transformação essa materializada em processos, sistemas e tecnologias para permitir uma massificação do trabalho remoto em toda a organização. Esta transformação, além de processos e tecnologias, deve envolver também pessoas.

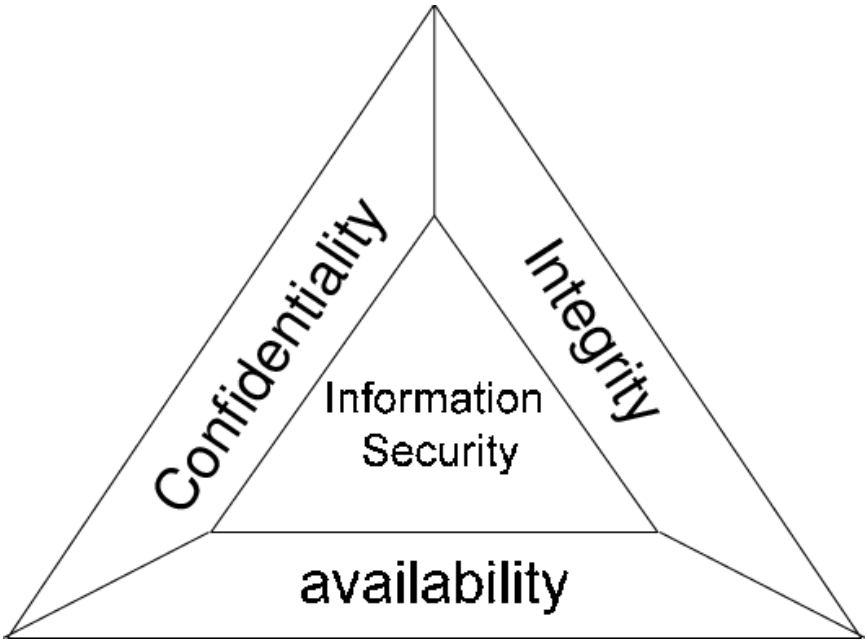
O contexto desta transformação, com a sua rápida mudança para um ambiente de trabalho remoto, criou uma pressão extra nas áreas de Segurança de Informação.

2. O Significado e a Significância da Segurança da Informação

Comecemos primeiro, servindo-nos do trabalho de Joseph Boyce[1], por referir a definição e importância da Segurança da Informação.

Segurança da Informação é todo o processo para a proteção e defesa da informação assegurando a sua Confidencialidade, Integridade e Disponibilidade[2] (DIC) ou na sigla em inglês CIA.

Figura 1



Na sua base a Segurança da Informação (SI) envolve a proteção dos direitos de pessoas e organizações. A SI permite às organizações a proteção dos seus direitos num meio concorrencial em que a informação sendo um ativo importante é também um elemento omnipresente no dia a dia das organizações desde a gestão às operações. A SI

1 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.
2 Estas são as três propriedades que de modo mais generalizado são reconhecidas. No entanto existem outras abordagens em que são referidas também as propriedades de **Não Repúdio** e **Autenticação**.

permite também às organizações a capacidade de proteger os direitos de outras entidades com quem interagem. Estas entidades incluem colaboradores, clientes (consumidores dos seus produtos) atuais e potenciais futuros clientes, fornecedores e outras organizações com quem se associem em resultado de parcerias ou *joint ventures*.

3. A Sociedade da Informação

A terceira Revolução Industrial ou Revolução Digital permite nos fins do século 20 a evolução para uma Sociedade da Informação. A chamada quarta Revolução Industrial ou Indústria 4.0 veio na última década dar uma importância acrescida às várias questões e desafios da Sociedade da Informação.

Dos vários desafios identificados a nível político, económico, social e organizacional destaca-se o desafio a nível social da vigilância, questões de confiança e preocupação da privacidade.

A nível organizacional destacam-se os desafios associados a: Problemas de segurança nas Tecnologias de Informação (TI) agravados pela necessidade ade abertura e conectividade de sistemas de produção anteriormente em ambiente fechado. Confiabilidade e estabilidade indispensáveis para todos os sistemas dependentes das TI, mas crítico em sistemas como por exemplo em M2M (*machine-to-machine communication*). Manutenção da Integridade da informação e dos processos de produção. Proteção da confidencialidade da informação. Neste último desafio destaca-se que a nível organizacional há a necessidade não só da proteção da propriedade intelectual, mas também da proteção dos dados pessoais de todos os envolvidos na organização, funcionários, clientes e outros envolvidos em parcerias[3].

A Sociedade da Informação está em todos os setores do quotidiano!

A atual Sociedade da Informação assente na crescente importância da informação e dos processos e meios que aceleram a disponibilidade da mesma tem vindo a potenciar

3 Wikipédia Indústria 4.0

um vasto com junto de melhorias, entre as quais se realçam os contributos para as organizações e sua gestão e também para as infraestruturas e a cidadania.

Temos presenciado, devido à valorização da informação, uma grande evolução nos processos de gestão e de governança.

As infraestruturas tecnológicas e os Sistemas de Informação (SI) permitem às organizações gerar vantagem competitiva sobre potenciais competidores. Assim a economia já não dispensa estes sistemas e infraestruturas que aumentam diretamente a sua cadeia de valor.

Também as chamadas infraestruturas críticas, privadas ou públicas, como telecomunicações, banca e finanças, transportes, energia, água, serviços de emergência, assentam cada vez mais em SI e Tecnologias de Informação e Comunicação (TIC), tornando-se deles dependentes. Aliás, as infraestruturas complexas são mais fáceis de gerir com computadores e sistemas operativos, aplicações e protocolos de redes comuns.

Paralelamente, a Sociedade de Informação traz novos desafios no que respeita à segurança[4].

Paradoxalmente, a conectividade que é uma vantagem é também o maior problema da segurança. O seu funcionamento em rede aberta, sem delimitação de fronteiras físicas, as relações de dependência e interdependência entre infraestruturas críticas, as vulnerabilidades de cariz tecnológico e a exposição a ações malévolas ou mesmo de menores cuidados de utilização, torna o ciberespaço muito exposto a novas vulnerabilidades e ameaças, algumas de natureza disruptiva.

Figura 2

4 Cibersegurança: das preocupações à ação - IDN Instituto da Defesa Nacional

As questões e soluções inerentes à Segurança da Informação baseiam-se em tecnologia, processos e pessoas e devem resultar duma análise, com identificação e avaliação, do valor da informação a proteger. Como é comum designar deve identificar-se quais são as "joias da coroa" da organização, fazer a respetiva avaliação e decorrente desse valor desenvolver e implementar as respetivas soluções.

4. Segurança da Informação e Cibersegurança

Os desafios inerentes à Segurança da Informação são também abordados na área da Cibersegurança.

Na definição do CNCS[5]:

"Cibersegurança - *Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem*."

"Segurança da Informação - *Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento,*

5 https://www.cncs.gov.pt/recursos/glossario/

processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças."

Conforme as normas e padrões de referência internacional utilizados assim também se utiliza mais uma definição ou outra.

As normas ISO 2700x são o padrão e a referência internacional para a gestão da Segurança da informação, e definem os requisitos e orientações para o desenho e implementação nas organizações de um Sistema de Gestão de Segurança da Informação (SGSI) ou ISMS (Information Security Management System)[6].

Além do ISO 2700x temos desde 2014 do NIST dos Estados Unidos a publicação da Estrutura de Segurança Cibernética NIST CSF (NIST Cyber Security Framework), que fornece uma estrutura de política de orientação sobre segurança de computadores, mais orientada para a proteção das organizações privadas americanas em relação a ciber ataques[7].

Não obstante a tendência recente que apresenta uma utilização crescente do termo Cibersegurança em detrimento de Segurança da Informação, da análise das definições de segurança da informação e ciber segurança produzidas pelos organismos europeu ENISA[8], americano CNSS[9] e organismos de certificação como o ISACA[10] entende-se a definição de Segurança da Informação como mais abrangente em relação à definição de Ciber Segurança.

6 https://www.27001.pt/
7 https://www.nist.gov/cyberframework
8 https://www.enisa.europa.eu/
9 https://www.cnss.gov/
10 https://www.isaca.org/

5. Impacto da Pandemia Covid-19

O dia 18 de março de 2020 fica marcado para sempre na história da democracia portuguesa. Foi a primeira vez que um Estado de Emergência foi decretado[11]. O anúncio deste estado de exceção indica que a situação "que se vive e a proliferação de casos registados de contágio de COVID-19 exige a aplicação de medidas extraordinárias e de caráter urgente". Uma das medidas indica, de forma sucinta, que todos as ocupações que possam ser feitas em trabalho remoto, ou teletrabalho, o devem ser feitos.

Nas duas semanas que antecederam o decreto do Estado de Emergência, várias empresas começaram a colocar os seus colaboradores em casa. Alguns colocaram todos os seus colaboradores a trabalhar a partir de casa; outros apenas uma parte para diminuir o risco de contágio na empresa. Certo é que, a partir de 18 de março, a larga maioria dos colaboradores passou a fazer o seu trabalho a partir de sua casa.

Passando de uma situação em que a força de trabalho estava localizada, na sua maioria, no perímetro restrito das instalações da organização para a situação oposta em que a maioria se encontra num ambiente de trabalho remoto.

Este contexto criou uma pressão extra nas áreas de cibersegurança.

O conceito de vírus informático surgiu pela primeira vez referido em 1984 num artigo de Fred Cohen[12]. O isolamento ou a menor conectividade possível dos sistemas informáticos ao mundo era a medida mais adequada para combater essa nova ameaça de infeção de vírus informático. Coincidentemente aquilo que resultava em 1984, e de certa forma ainda hoje, para segurança informática é também a medida recomendada, e imposta, no combate à pandemia do Covid19.

Aqui surge o desafio, no combate às ameaças biológica e informática, enquanto para uma boa proteção de ciber ataques a melhor forma é trabalhar a partir de infraestruturas com arquiteturas de segurança robustas, para uma boa proteção em relação ao Covid-19 o melhor é ficar em casa utilizando os equipamentos informáticos e as redes de comunicação pessoais para uso profissional. O Covid-19 fez com que milhões de

11 https://www.presidencia.pt/?idc=22&idi=176060
12 Herb Lin, 2020. Cybersecurity Lessons from the Pandemic

pessoas passassem a aceder às redes e servidores das suas empresas e organizações a partir de casa e através de redes com níveis de segurança inferiores.

Como publicado no boletim de maio de 2020 do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), entre fevereiro e março de 2020, o número de incidentes registados pelo CERT.PT – serviço que coordena a resposta a incidentes de cibersegurança no ciberespaço de interesse nacional – aumentou 84% e, em comparação com o número de incidentes registados em março de 2019, o aumento foi de 176%[13].

Citando Dorit Dor, Vice Presidente da *Products at Check Point Software Technologies*:

> "*A pandemia COVID-19 descarrilou a atividade normal de praticamente todas as organizações, obrigando-as a pôr de lado os planos estratégicos de negócio que tinham já delineado e a adotar rapidamente medidas que garantam a conectividade remota em larga escala para a sua força de trabalho*."

> "*Uma das poucas coisas previsíveis sobre a cibersegurança é que os agentes maliciosos procurarão sempre tirar proveito próprio de grandes eventos ou mudanças – como a COVID-19 ou a introdução do 5G*."

Um dos grandes desafios que as organizações atualmente enfrentam passa por encontrar formas de conciliar o trabalho remoto dos seus colaboradores com a segurança dos dados críticos, mais expostos a riscos online devido à dispersão geográfica de quem está em modo de teletrabalho.

Com a movimentação de centenas de milhar de trabalhadores para as suas casas moveu-se também o perímetro de segurança da respetiva empresa. E se tivermos em conta que estas alterações serão o novo normal, podemos inferir que os dados críticos das organizações estão significativamente mais expostos a ciberataques.

13 https://www.cncs.gov.pt/content/files/boletim_observatorio_maio2020.pdf

A solução passa, claro, pela adoção de soluções de segurança que protejam as infraestruturas, o software e a informação. Mas é hoje necessário olhar para estes riscos de uma forma transversal, através de sistemas de monitorização fiáveis, sistemáticos e que forneçam recomendações para uma atuação proativa de mitigação desses mesmos riscos.

Além disso, é essencial não limitar os utilizadores naquilo que é a sua ação normal de trabalho, disponibilizando em paralelo as ferramentas adequadas para o acesso aos sistemas e aos dados e assegurando sempre a proteção devida – sejam propriedade intelectual ou dados ao abrigo do RGPD.

6. Mudança do Perímetro de Defesa

Segundo Joseph Boyce, numa perspetiva de Segurança da Informação os serviços e mecanismos de segurança devem abranger um vasto campo de equipamentos de TI da organização. A diversidade é a base duma estratégia de Defesa em Profundidade. Essa diversidade pode ser alcançada com a implementação de serviços e mecanismos de segurança em estações de trabalho, as chamadas workstations, desktops, laptops, como em servidores, routers, firewalls, como apenas alguns exemplos.

"*Organizational computing environment boundary protection*"[14]. Estações de trabalho e servidores localizados nas instalações da organização têm de ser protegidos tanto de ameaças internas como externas à organização e suas instalações. Assim os referidos equipamentos deverão ter implementados serviços e mecanismos de segurança tais como autenticação e controlo de acessos.

14 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

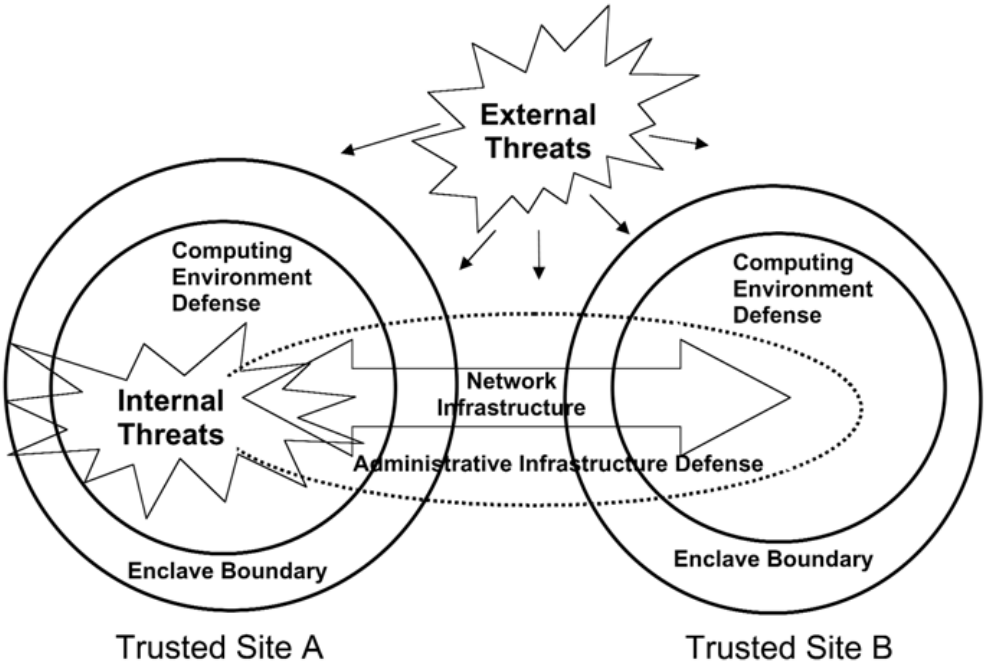


Figura 3[15]

Embora aqui neste ponto Joseph Boyce refira apenas equipamentos localizados nas instalações da organização, já no capítulo 3 refere as fronteiras físicas e virtuais numa organização.

Neste mesmo capítulo define também o conceito de ambiente de computação como tudo o que trabalha com qualquer ou todos os ativos do sistema de informação do enclave, enclave que define como uma área fisicamente protegida dentro da organização, no entanto adiciona que neste enclave pode incluir-se também um laptop com uma sessão remota a partir dum hotel por parte dum funcionário em viagem. Nesta altura ainda não existia esta realidade de trabalho remoto massivo.

Mudando para um trabalho remoto, em casa, mudou-se assim também o perímetro de defesa ou perímetro de segurança da respetiva empresa.

Esta mudança do perímetro de defesa coloca os seguintes desafios nas áreas de cibersegurança:

15 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

• Explosão "BYOD – *Bring your own device*" – Muitos colaboradores não tinham dispositivos (ex.: *laptops* ou *smartphones*) atribuídos pela empresa para uso *off-site* no momento do confinamento.

• Ambiente de computação remoto – As organizações não têm controlo sobre o ambiente de computação remoto dos seus colaboradores.

• Acesso remoto seguro – A maioria das empresas simplesmente não estava pronta para um mundo onde a maioria dos colaboradores não tem acesso remoto seguro às aplicações corporativas.

• A ameaça interna – Os ambientes de competitividade económica continuarão a contribuir para um aumento no volume de ameaças internas.

• Processos "*ad hoc*" inseguros – Foram executados processos de desenvolvimento rápidos para suportar esta nova realidade, ou mesmo para aumentar o volume de negócios em canais digitais, que infelizmente num número significativo de organizações, eventualmente devido à urgência, não passaram por nenhuma validação da área de cibersegurança.

Todos estes desafios têm implícitos uma panóplia de riscos que não sendo novos na sua maioria, são, no entanto, exacerbados pela procura crescente de soluções de trabalho remoto e pela necessidade das organizações em concretizar uma rápida transformação digital de modo a fazer face a esta nova realidade de trabalho remoto massivo.

7. Como será o novo normal?

Em resultado da análise duma plêiade de estudos constata-se que todos convergem para uma conclusão: O trabalho remoto vai manter-se e vai intensificar-se[16][17][18].

No entender dos investigadores da *Check Point*, os efeitos causados pelas mudanças introduzidas pela pandemia COVID-19 continuarão a ser o foco das equipas de TI e de segurança das organizações. Um estudo recente da Gartner estima que 81% das empresas adotaram massivamente o trabalho remoto, sendo que 74% pondera esta opção permanentemente[19].

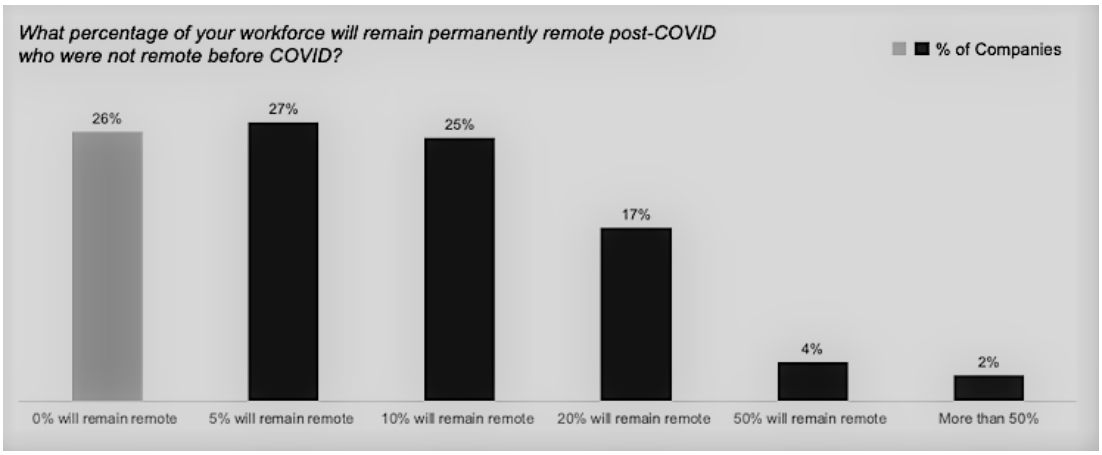


Figura 4 [20]

A *Check Point* alerta ainda para as repercussões que a emergência de ataques ransomware e de botnets terá no que respeita a capacidade das empresas de proteger as redes 5G e a crescente conetividade entre dispositivos.

Como foi apresentado anteriormente, tanto a explosão de BYOD como o desconhecido ambiente de computação remoto dos seus colaboradores são dos principais

16 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf
17 https://blog.sage.hr/post-covid-future-of-work-trends/
18 https://businessfacilities.com/2020/06/even-after-covid-19-execs-expect-remote-work-trend-to-continue/
19 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
20 https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/cohotrm.png

desafios das áreas de cibersegurança para este novo normal de permanência de trabalho remoto.

Assim identificam-se como fundamentais os seguintes 3 processos para assegurar a adequação das organizações ao novo cenário de trabalho remoto massificado:

- Garantir que as equipas de Tecnologias de Informação implementam as políticas e diretrizes de segurança corporativa para os "BYOD – *Bring your own device"*.
- Rever e adequar as regras de firewalls corporativas para acesso remoto, monitorizar e analisar os Comportamentos de Utilizadores e Entidades (UEBA- *User and Entity Behavior Analytics*).
- Restringir o acesso à rede corporativa apenas a equipamentos pessoais aprovados.

As abordagens atrás mencionadas irão impulsionar o interesse renovado em tecnologias que permitam acesso remoto seguro. Das tecnologias disponíveis atualmente algumas já existiam há bastante tempo, mas tiveram, no entanto, fraca adesão no passado devido a questões de complexidade e custo de implementação, agora, devido à crescente evolução para *Cloud* estão assim novamente com grande potencial de utilização no sentido de contribuir para as abordagens referidas anteriormente.

Destacam-se[21]:

• "VDI – *Virtual Desktop Infrastructure*" e "DaaS – *Desktop as a Service*":

• "IAM – *Identity and Access Management*";

• *Cloud computing*.

21 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf

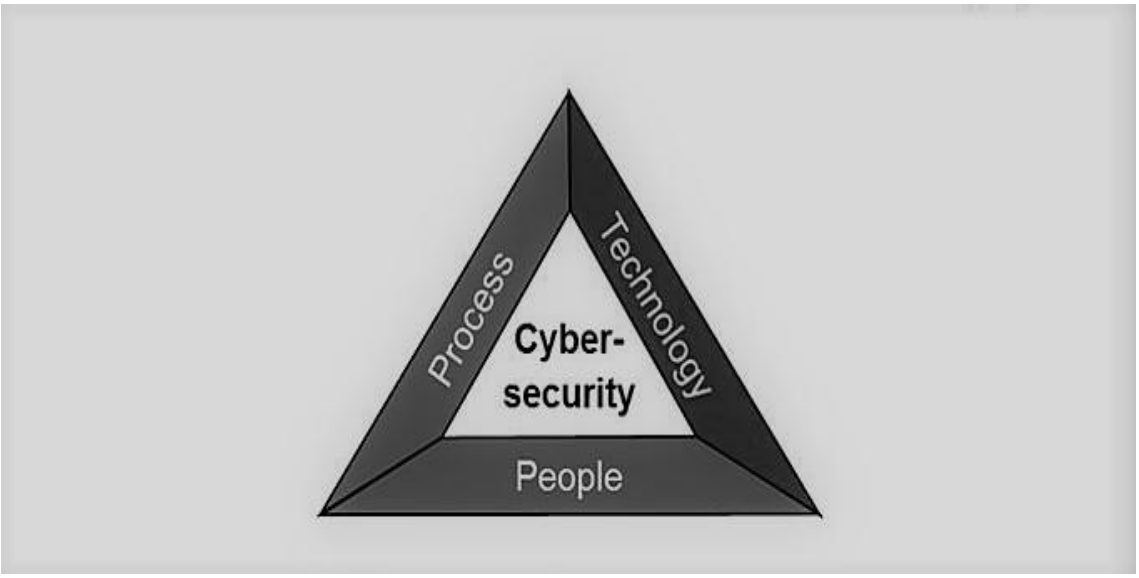
Conclusões

As organizações da área das TI, algumas já referidas como "*cloud-native*", tinham em geral já estabelecidos a maioria dos processos e tecnologias necessários para o trabalho remoto. Neste caso a mudança para um trabalho remoto massificado pode ser encarado como mais um passo ou apenas uma evolução nesse processo. As organizações com mais dificuldades são as que ainda têm de evoluir no seu grau de maturidade na Segurança da Informação.

Segundo um estudo da *EU Science HUB*[22], em vários países da União Europeia mais de metade das pessoas atualmente em trabalho remoto nunca tinham tido essa experiência anteriormente.

O desempenho e sucesso das organizações no geral e também neste tema da Segurança da Informação em particular tem como base a articulação da tríade: Pessoas, Processos, Tecnologias.

Figura 5



22 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf

Então, que devem as organizações, e seus colaboradores, fazer para a proteção da sua informação e dados críticos?

Da análise dos vários estudos[23] [24] [25] [26] e das muitas recomendações analisadas sintetizaram-se as similares e agregaram-se nas 3 vertentes de processos, tecnologias e pessoas.

Portanto muito resumidamente teremos:

Processos

• Assumir que as ameaças vão existir

• Definir uma política para o trabalho remoto

• Encriptar Informação/Dados críticos

Tecnologias

• Especificar a lista de equipamentos de trabalho remoto e implementar as respetivas medidas de segurança

• Usar autenticação, controlos e privilégios de acesso apropriados para cada utilizador

• Usar uma VPN

23 https://www.cmswire.com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/
24 https://techbeacon.com/security/pandemic-your-remote-workforce-9-ways-stay-secure
25 https://www.cybereason.com/blog/cyber-security-tips-for-allowing-employees-to-work-from-home
26 https://memory.ai/timely-blog/cyber-security-for-remote-workers

Pessoas

• Fomentar a sensibilização (*awareness*) dos funcionários para o problema da segurança da informação.

• Aumentar também o conhecimento técnico dos funcionários em relação a esta mesma problemática da segurança da informação.

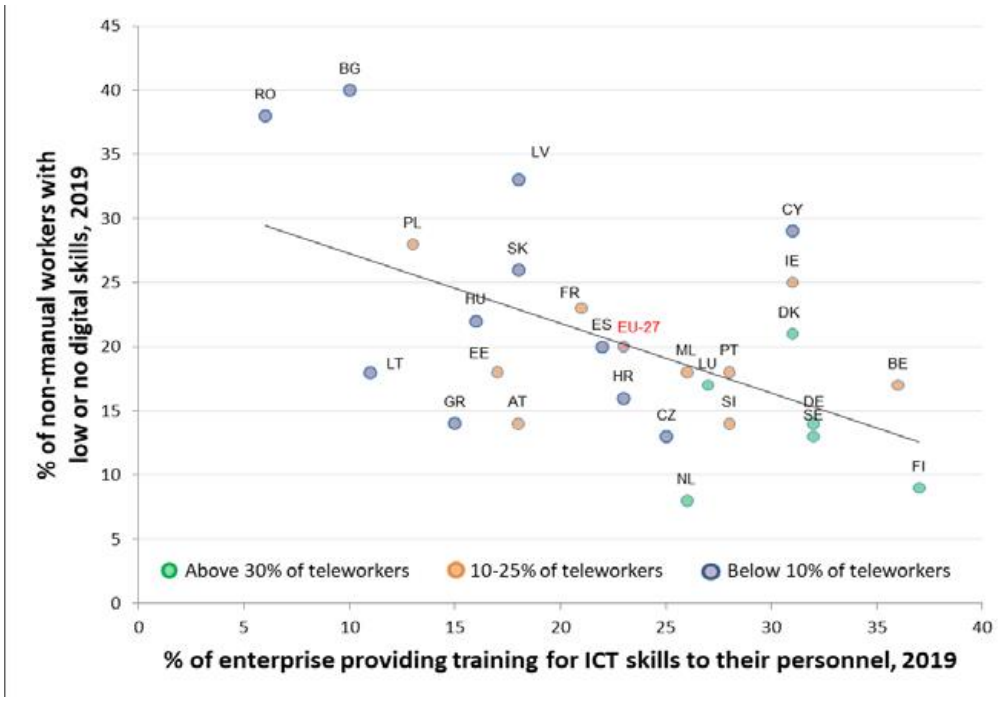
Ou seja: Treinar, treinar, treinar. Sensibilizar, sensibilizar, sensibilizar.

As tecnologias existem, evoluirão muitas das atuais, surgirão novas e desaparecerão algumas. Os processos também já existiam, e evoluirão também tal como as tecnologias.

São as pessoas o elo mais fraco nesta tríade.

Neste gráfico apresentado abaixo, do mesmo estudo da EU Science HUB JRC[27] já referido também anteriormente, constatam-se as diferenças entre competências digitais e formação providenciada pelas empresas nos diferentes estados-membro e consoante as diferentes políticas de trabalho.

Figura 6 [28]



27 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf
28 Figure 11: Digital skills, ICT training and telework: jrc120945_policy_brief_-_covid_and_telework_final.pdf.

Neste gráfico temos como média da EU-27 que 20% dos colaboradores (em trabalho não manual) têm nenhumas ou baixas competências digitais e menos de 25% das empresas providenciam formação em competências digitais.

Nota-se também a influência positiva das empresas com mais de 30% dos colaboradores em trabalho remoto, todas no quadrante inferior direito do gráfico, em contraste com a situação inversa das empresas com menos de 10% dos colaboradores em trabalho remoto, mais no quadrante superior esquerdo do gráfico.

Assim, esta crise provocada pela pandemia do Covid-19 com as consequentes restrições impostas sendo uma delas o trabalho remoto massivo forçado, deve ser aproveitada no sentido da transformação digital que foi forçada também em muitas das empresas e acelerada noutras que já a tinham em curso ser, entretanto, agora com o devido tempo e ponderação, analisada e aperfeiçoada.

Essa análise e aperfeiçoamento deve incidir não só nos processos e tecnologias como também nas pessoas. Será mais difícil ter uma transformação digital bem-sucedida e também uma Segurança da Informação bem implementada sem as respetivas competências nas pessoas.

Parafraseando Winston Churchill: "*Never let a good crisis go to waste*".

Bibliografia

Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

Caldas, Alexandre, e Vicente Freire. "Cibersegurança: das preocupações à ação - IDN Instituto da Defesa Nacional." s.d.

check-point-softwares-cyber-security-predictions-for-2021. s.d. https://www.checkpoint.com/press/2020/check-point-softwares-cyber-security-predictions-for-2021-securing-the-next-normal/.

"Ciberseguranca eciberdefesaemtemposdepandemia_IDNBrief_N_32_Julho_2020." s.d.

cmswire. *6-ways-to-keep-employer-data-secure-when-working-remotely.* s.d. https://www.cmswire.com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/.

CNCS. *boletim_observatorio_maio2020.* s.d. https://www.cncs.gov.pt/content/files/boletim_observatorio_maio2020.pdf.

—. *Cibersegurança, Glossário.* s.d. https://www.cncs.gov.pt/recursos/glossario/.

CNSS. *CNSS.* s.d. https://www.cnss.gov/.

cybereason. *cyber-security-tips-for-allowing-employees-to-work-from-home.* s.d. https://www.cybereason.com/blog/cyber-security-tips-for-allowing-employees-to-work-from-home.

Deloitte. "gx-covid-19-cyber-and-the-remote-workforce." s.d. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf.

ENISA. *ENISA.* s.d. https://www.enisa.europa.eu/.

Facilities, Business. *Business Facilities - Surveys & Research.* s.d. https://businessfacilities.com/2020/06/even-after-covid-19-execs-expect-remote-work-trend-to-continue/.

Gartner. *Gartner press-releases.* s.d. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2.

ISACA. *ISACA.* s.d. https://www.isaca.org/.

ISO. *ISO.* s.d. https://www.iso.org/news/ref2266.html.

—. *ISO 27001 pt.* s.d. https://www.27001.pt/.

JRC, EU Science Hub. "Telework in the EU before and after the COVID-19: where we were, where we head to." *European Commission > EU Science Hub.* s.d. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf.

Lin, Herb. *Cybersecurity Lessons from the Pandemic.* s.d. https://www.lawfareblog.com/cybersecurity-lessons-pandemic-or-pandemic-lessons-cybersecurity.

memory.ai. *cyber-security-for-remote-workers.* s.d. https://memory.ai/timely-blog/cyber-security-for-remote-workers.

NIST. *NIST CSF.* s.d. https://www.nist.gov/cyberframework.

post-covid-future-of-work-trends. s.d. https://blog.sage.hr/post-covid-future-of-work-trends/.

Presidencia. *Presidencia.* s.d. https://www.presidencia.pt/?idc=22&idi=176060.

techbeacon. *pandemic-your-remote-workforce-9-ways-stay-secure.* s.d. https://techbeacon.com/security/pandemic-your-remote-workforce-9-ways-stay-secure.