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

CYBERLAW by CIJIC

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*

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.

sabem que já foram atacadas e as que ainda não o sabem (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

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?

---

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.

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

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).

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. *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?

---

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).

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

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.

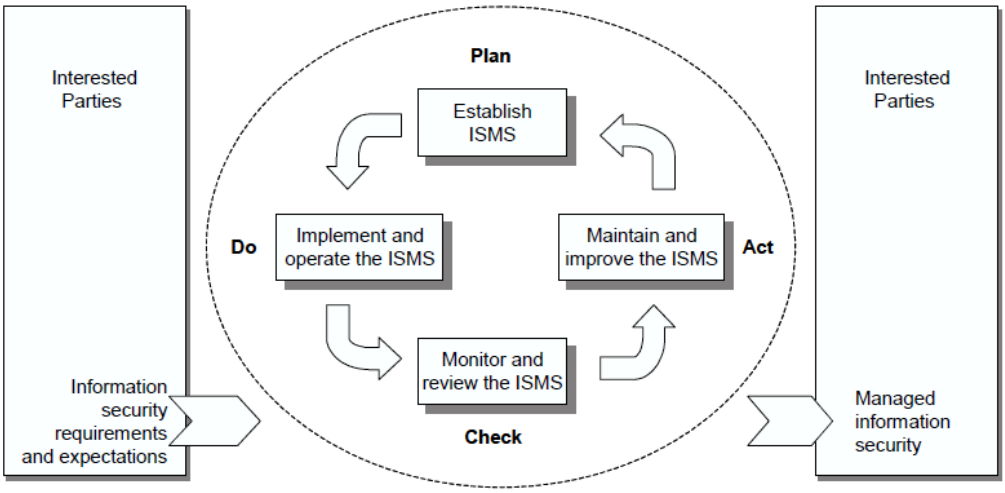

Figure 1 — PDCA model applied to ISMS processes

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