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

CYBERLAW by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

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

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

---

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

---

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)****».***

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma 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 justíssimo: - Muito Obrigado.

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

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?
18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

DOUTRINA

CYBERLAW by CIJIC

CIBERSEGURANÇA NO SETOR MARÍTIMO

A. GAMEIRO MARQUES *

* Diretor-Geral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança, Oficial da Marinha Portuguesa.

RESUMO

No âmbito da Conferência realizada em Dezembro de 2019 na Faculdade de Direito da Universidade de Lisboa, sobre Cibersegurança no Setor Marítimo, partilhamos algumas considerações sobre um tema que nos é especialmente grato. Neste conspecto, consideramos pertinente adiantar desde logo o repto seguinte: "Ao longo dos tempos a história tem-nos mostrado que sem segurança não há desenvolvimento sustentado. A segurança, incluindo a cibersegurança, é uma responsabilidade coletiva onde todos os atores, sejam públicos ou privados, devem cooperar para que juntos, possamos estar mais preparados para as ameaças que conhecemos e sobretudo para as que desconhecemos. Tal como noutros setores da sociedade, também no setor marítimo cada vez mais dependemos da tecnologia para viver como vivemos.»

***Palavras-Chave**: Cibersegurança, tecnologia; Setor Marítimo; Valor estratégico; "security by design"; "safety"*

1. INTRODUÇÃO

Começo por agradecer o gentil convite que me foi dirigido pelo Sr. Professor Eduardo Vera Cruz, para proferir esta comunicação subordinada ao tema "Cibersegurança no Setor Marítimo", que congrega duas áreas que muito me dizem: a cibersegurança, por ser aquela em relação à qual detenho a responsabilidade de Direção superior da entidade do Estado onde funciona o Centro Nacional de Cibersegurança, a quem incube a coordenação da resposta a incidentes de cibersegurança, incluindo a capacitação da sociedade para os desafios que o mundo digital no aporta; e o mar, por ser, desde há algumas dezenas de anos Oficial da Marinha Portuguesa, e em relação ao qual mantenho um incessante fascínio, interesse e gosto por tudo o que com ele se relaciona e por ele estar, efetivamente, na base da nossa identidade enquanto Estado Nação e ainda por constituir um recurso fundamental para o nosso desenvolvimento económico. Assim, é com redobrado gosto que me encontro nesta prestigiada entidade para partilhar algumas reflexões sobre o tema.

Agradeço, ainda, a todos os presentes. O estarem aqui é para mim um claro sinal do interesse que estes assuntos vos suscitam, uma vez que, sendo tão atuais, são cada vez mais condicionadores da forma como vivemos, incluindo o modo como as democracias e assim os direitos liberdades e garantias dos cidadãos se exercem. E este assunto, que poderia ser tema para um outro debate, é cada vez mais relevante e potencialmente determinante quanto à forma como cada vez mais os poderes detidos, quer por Estados quer por grandes empresas transnacionais, se irão exercer ao nível geoestratégico.

No início deste ano tive o grato prazer de ouvir, com muito interesse e atenção, na Academia de Marinha uma alocução proferida pelo Sr. Professor Dr. António Barreto intitulada "O Mar como património". Reli a sua comunicação e retive algumas ideias que gostaria de trazer à colação: o Sr. Professor afirmou que, para a sua definição de identidade, contava com "a natureza, a geografia, o património e a história". Na sua alocução referiu ainda que "a singularidade de Portugal (e de qualquer outro país) reside na combinação única da sua natureza com a geografia e a história. A geografia mais o património de um

país são, em grande parte, a sua identidade. O património … é toda a criação cultural, técnica, artística e ideológica de um povo." A questão que aqui coloco para reflexão é a seguinte: será que poderemos reforçar a nossa singularidade e o nosso património identitário através do Mar, no contexto da rápida evolução que o digital constantemente nos aporta, mais concretamente no âmbito do tema desta conferência? Se sim, como poderemos fazer isso?

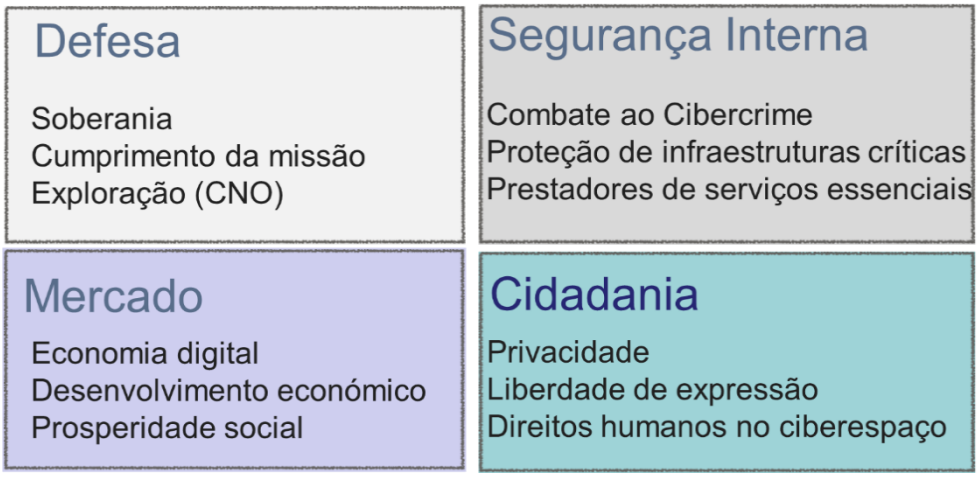
2. ENQUADRAMENTO CONCEPTUAL

Do ponto de vista doutrinário, o Mar possui cinco dimensões estratégicas, a saber: a ambiental, a política, a económica, a social e a securitária. A **dimensão ambiental** contempla as características intrínsecas do Oceano inerentes ao facto de 70% da terra ser coberta com água, ser um natural sumidouro de Dióxido de Carbono, constituir uma cada vez mais vital fonte de Oxigénio, um determinante regulador do clima, para além de ser uma preciosa fonte de biodiversidade. A **dimensão geopolítica** por constituir um espaço de afirmação e de disputa de poder, que povos, ao longo da história da humanidade (como foi o nosso caso nos séculos XV e XVI), foram conquistando para afirmação planetária da sua influência geoestratégica. A **dimensão económica**, uma vez que 90% do comércio mundial se faz pelo mar, as comunicações que materializam 97 % da Internet tal como hoje a conhecemos estão baseadas em milhares de Km de cabos submarinos (em que Portugal representa um local particularmente de destaque por ser o único País da União Europeia ligado por este meio à maioria dos continentes), para além de ser uma enorme fonte de energia e de recursos naturais da mais diversa índole. A **dimensão social** porque um terço da população mundial vive em zonas costeiras, 80% das mega cidades estão implantadas ao longo das zonas ribeirinhas e cerca de 30% dos empregos existentes estão direta ou indiretamente ligados à economia do Mar. Finalmente, a **dimensão securitária**, que contempla atividades desde as que endereçam situações de "safety", de baixo espetro de intensidade e normalmente não intencionais, até às de Defesa Naval, numa lógica multidimensional, eventualmente suscetíveis de ser enquadradas no conceito de "ameaças híbridas", atualmente consagrado quer na doutrina da OTAN quer na da EU.

Por outro lado, o ciberespaço é um domínio que hoje em dia é utilizado quer por Estados quer por organizações supranacionais, para afirmação do seu poder geoestratégico. E é neste contexto que conceptualmente podemos afirmar que a cibersegurança possui 4 dimensões: a de Defesa, como espaço ou domínio de exercício da soberania e da proteção dos interesses de um Estado no ciberespaço, designadamente através do planeamento e condução de *Computer Network Operations*; uma segunda, no âmbito da "segurança interna" que contempla o combate ao cibercrime, a proteção de infraestruturas críticas e prestadores de serviços essenciais ao saudável funcionamento da sociedade; uma terceira, a dimensão económica, como acelerador e facilitador da economia digital, uma vez que bem

sabemos que não existe desenvolvimento económico sustentável sem segurança, e finamente a dimensão de cidadania, com enfoque na privacidade do cidadão, nos seus direitos liberdades e garantias, incluindo a liberdade de expressão. Esta é, talvez hoje, a dimensão mais ameaçada, na medida em que existem reiteradas evidências de Estados (ou entidades por si patrocinadas), que cada vez mais usam o ciberespaço para controlo e limitação da liberdade dos seus cidadãos.

As dimensões da cibersegurança



Vejamos, de seguida, como é que as duas se relacionam, i.e., como é que as dimensões da visão estratégica do mar se ligam com as dimensões da cibersegurança:

Valor estratégico do Mar vs Cibersegurança

		CIBERSEGURANÇA			
	Dimensões	**Defesa**	**Seg. Interna**	**Economia**	**Cidadania**
VALOR EST. DO MAR	**Ambiental**				
	Geopolítica				
	Económica				
	Social				
	Securitária				

Ainda que sem a profundidade de uma análise científica, julgo que fica claro que as dimensões do valor estratégico do Mar têm uma profunda relação com as dimensões da cibersegurança, o que indicia que, quaisquer iniciativas enquadrados no primeiro, devem ser acompanhadas dos mecanismos adequados nas componentes da cibersegurança, para que o uso do mar não fique quartado de todo o seu potencial, sobretudo quando cada vez mais as atividades neste importante setor dependem do digital e assim do ciberespaço.

3. CARACTERIZAÇÃO DO SETOR MARÍTIMO E OS CIBERATAQUES NESTE SETOR

Quando neste contexto falamos do Mar referimo-nos concretamente a três componentes do setor marítimo: (i) as infraestruturas portuárias e de vigilância costeira incluindo as respetivas autoridades; (ii) os navios em geral, em particular os que possuem guarnições multinacionais, cujos armadores são muitas vezes proprietários de embarcações que arvoram bandeiras de conveniência; (iii) e as cadeias logísticas que são responsáveis não só pelo abastecimento dos próprios navios, como pela garantia que as mercadorias são transportadas da sua origem ao cliente de forma segura e determinística.

As infraestruturas portuárias são complexas e têm a sua atividade ancorada em sistemas de IT bastante elaborados, que, sendo fundamentais para as atividades dos portos, não foram concebidos, de uma forma geral, com o princípio da "security by design". O mesmo acontece com os sistemas de vigilância marítima, desde os costeiros aos portuários.

Os navios são cada vez mais concentrados de tecnologia da mais diversa índole e origem, como forma de incrementar os respetivos automatismos e assim diminuir a necessidade de guarnições numerosas, incrementando, desta forma, a rentabilidade da atividade económica. Como é consabido, já existem experiências de operações com navios de dimensões assinaláveis sem qualquer ser humano a bordo para respetiva operação.

Para aumentar a sua eficiência, a cadeia logística recorre a vários tipos de sistemas de informação e comunicação, desde os que permitem efetuar o rastreamento dos contentores na zona portuária propriamente dita até aos que, como a Janela Única Logística (JUL), permitem efetuar o processamento do navio e respetiva carga de forma desmaterializada, envolvendo as diversas entidades necessárias ao respetivo tratamento ao longo de todo o processo.

Se a este complexo contexto adicionarmos a baixa sensibilidade da comunidade marítima para a importância da cibersegurança no setor; a falta de um sólido corpo de recomendações e standards que se encontra em desenvolvimento, mas ainda não é exaustivo; a fragmentação da governação dos assuntos relacionados com este setor; a falta de uma abordagem transversal aos ciber riscos, que são dilatados pela diversidade dos atores em jogo;

e finalmente a inexistência de incentivos económicos à implementação de boas práticas de cibersegurança no setor marítimo, temos o que é necessário para que as coisas possam não correr satisfatoriamente.

Os factos são demonstrativos disto mesmo (mostrar com os tipos de ataques mais comuns no setor e os mais recentes e significativos – 3 slides). O que mais nos deve preocupar é que, para além do grave impacto económico e reputacional que tal pode trazer a um armador, a um porto, enfim a um País, um incidente de cibersegurança perpetrado numa grande instalação portuária ou num navio pode provocar um problema ainda maior de "safety", com danos ambientais e mesmo perda de vidas humanas. Por outras palavras, estamos convencidos que negligenciar estes assuntos poderá impactar negativamente o valor estratégico do mar em todas as suas dimensões. É, por isso, necessário agir de forma sistemática, estruturada e perseverante.

Consciente deste facto, a Agência da União Europeia para a segurança das redes e da informação (ENISA) publicou em dezembro de 2011 um relatório que aferiu o "estado da arte" na união no que à cibersegurança no setor marítimo diz respeito. Já naquela altura o documento mostrava evidências de que o setor sofria de problemas de diversa índole, que o tornavam muito vulnerável a ataques perpetrados por pessoas ou organizações mal-intencionadas.

Desde então, várias iniciativas da parte da UE ocorreram, visando mitigar os riscos de segurança (que incluía a cibersegurança), das quais destacaria a publicação, em 24 de Junho de 2014 da EU Maritime Security Strategy[1], cujo plano de ação foi divulgado em 16 de Dezembro desse mesmo ano[2]. Posteriormente, foram desenvolvidos dois relatórios relativos ao seu estado de execução, em 22 de Junho de 2016[3], e 14 de Junho de 2017[4] respetivamente. Já em 26 de junho de 2018 foi publicado uma revisão do plano de ação original bem como as conclusões do Conselho sobre esse documento[5].

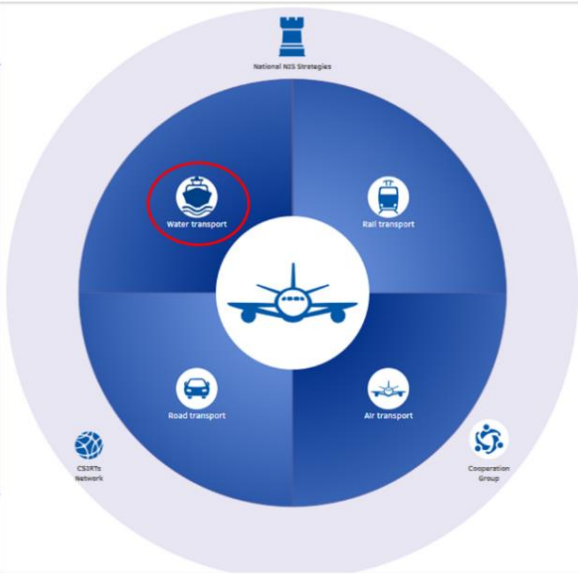
Da leitura deste conjunto de documentos pode-se apurar que o tema da cibersegurança se encontra contemplado, estando relacionado, quer com a *EU Cybersecurity Framework*,

1 https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en
2 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf
3 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/swd-2016-217_en.pdf
4 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/swd-2017-238_en.pdf
5 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf

anunciada pelo Presidente da Comissão Europeia em setembro de 2017 quer, mais importante ainda, com a Diretiva sobre a Segurança das Redes e dos Sistemas de Informação (Diretiva SRI) adotada pelo Parlamento Europeu em 6 de julho de 2016[67]. Esta é a primeira legislação da União Europeia sobre segurança do ciberespaço, que estabelece um conjunto de medidas para capacitar os Estados-Membros para proteger, prevenir, reagir e combater incidentes desta natureza. Entre outros objetivos, visa aumentar a cooperação na União nesta matéria e criar uma sólida cultura de segurança em sectores essenciais para a sociedade que dependam fortemente do domínio digital.

Diretiva relativa à Segurança das Redes e dos Sistemas de Informação (Lei 48/2018 de 13 de Agosto)

Setores	Subsetores	Tipo de entidades
	c) Transporte marítimo e por vias navegáveis interiores	– Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, tal como definidas, para o transporte marítimo, no anexo I do Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho[2], não incluindo os navios explorados por essas companhias
		– Entidades gestoras dos portos na aceção do artigo 3.º, ponto 1, da Diretiva 2005/65/CE do Parlamento Europeu e do Conselho[3], incluindo as respetivas instalações portuárias na aceção do artigo 2.º, ponto 11, do Regulamento (CE) n.º 725/2004, e as entidades que gerem as obras e o equipamento existentes dentro dos portos
		– Operadores de serviços de tráfego marítimo na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho[1]



https://www.enisa.europa.eu/news/enisa-news/enisa-releases-online-nis-directive-tool-showing-per-sector-the-national-authorities-for-operators-of-essential-services-and-digital-service-providers

O Anexo II da Diretiva (e também no anexo à Lei 46/2018 de 13 de agosto que a transpõe para a legislação nacional) elenca os serviços designados como "essenciais" para a sociedade, que incluem os transportes em geral e o transporte marítimo em particular. Todavia não contempla um dos mais importantes e também um dos mais difíceis componentes: os navios. Nem tão pouco fornece orientações específicas quanto à melhor forma de mitigar a governação fragmentada que se observa neste setor, o que já era um problema identificado no relatório da ENISA de dezembro de 2011.

6 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT
7 Transposta para a legislação nacional através da já mencionada Lei 46/2018 de 13 de agosto

Com a insistência de alguns estados membros, entre os quais Portugal, a ENISA voltou a debruçar-se sobre o estado da cibersegurança no setor marítimo, optando por uma abordagem segmentada: acabou de publicar e apresentar a 26 de novembro em Lisboa num workshop sobre cibersegurança no setor marítimo um relatório sobre a cibersegurança no subsetor portuário em 2019. Este relatório[8] identifica de forma concreta as maiores ameaças que o setor enfrenta no ciberespaço e caracteriza os vários cenários mais plausíveis de ocorrerem no contexto portuário, incluindo as técnicas e os procedimentos para lhes fazer face.

Relativamente aos navios, diversas entidades internacionais ligadas ao setor marítimo, das quais destacaria a *International Maritime Organiza*tion (IMO), o *Oil Companies International Marine Forum* (OCIMF), e a *International Maritime Contractors Association* (IMCA), desenvolveram e atualizaram documentação já existente sobre a segurança (security) a bordo dos navios, incluindo a cibersegurança ainda que sejam "orientações" e não regras a cumprir.

Por seu lado, a Comissão Europeia definiu que a cibersegurança no setor marítimo é uma prioridade estratégica[9]. Através do *NIS Cooperation Group*, no qual Portugal é representado pelo CNCS, aquela entidade lidera os trabalhos que esperemos venham dar origem a planos de ação concretos para tornar este setor, que tanto depende do digital, mais resiliente a ataques cibernéticos.

8https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

9 Svetlana Schuster, Dr. Nineta Polemi, Comissão Europeia, Reunião do Cooperation Group da CE, 4SET19

4. SITUAÇÃO EM PORTUGAL

A Lei 46/2018 de 13 de agosto efetuou a transposição da Diretiva SRI já mencionada. Esta legislação estabelece que o CNCS é o ponto focal para os assuntos de cibersegurança nos setores que prestam serviços essenciais à sociedade, entre os quais se encontra o setor dos transportes marítimos.

Neste âmbito, o Centro tem trabalhado com os reguladores de todas as áreas previstas naquela Lei na identificação dos respetivos operadores de serviços essenciais e do modelo que deverá enquadrar a respetiva regulação, a qual já se encontra em curso. Assim, foram identificadas e notificadas mais de um milhar de entidades das quais 11 pertencem ao setor dos transportes marítimos.

Uma vez que, de uma forma global, a atuação do CNCS se alicerça no princípio da subsidiariedade, estamos a trabalhar, em estreita colaboração com os reguladores do setor (AMT e DGRM), que o preconizado naquela diretiva e transposto na legislação nacional, seja cumprido e devidamente acompanhado. Neste enquadramento, iremos recomendar a aplicação de um modelo que já foi utilizado noutras áreas e que consiste na criação de um *Information Sharing and Analysis Center* (ISAC)[10] específico, desejavelmente endossado e apoiado pelo nível político, como por exemplo a Comissão Interministerial para os Assuntos do Mar (CIAM). O CNCS tem documentação produzida e experiência na ajuda à criação destes mecanismos em Portugal, e pode ser um facilitador da construção de algo congénere no nosso País. Todavia, considero que o nível de ambição deve ser maior. De facto, julgo que se deveria desenvolver um modelo de prestação de serviços colaborativo na comunidade marítima, mais concretamente com os portos nacionais, de modo a tornar as políticas e os procedimentos de segurança de informação coerentes e interoperáveis, incrementar a capacidade de recurso a fundos da UE (CEF-TELECOM) e otimizar o emprego de recursos humanos e financeiros (CAPEX e OPEX) na edificação e manutenção da capacidade de cibersegurança portuária.

10 https://www.cncs.gov.pt/cooperacao/isac/

Paralelamente, e como nação cuja identidade e singularidade está indelevelmente ligada ao Mar, julgo que nos fóruns internacionais, designadamente ao nível das instâncias europeias, Portugal deverá continuar a trazer e a perseguir os assuntos da cibersegurança no setor marítimo para agenda, pois assim estará a pugnar pelos seus interesses e a honrar a sua identidade e singularidade.

5. CONCLUSÕES

Ao longo dos tempos a história tem-nos mostrado que sem segurança não há desenvolvimento sustentado. A segurança, incluindo a cibersegurança, é uma responsabilidade coletiva onde todos os atores, sejam públicos ou privados, devem cooperar para que juntos, possamos estar mais preparados para as ameaças que conhecemos e sobretudo para as que desconhecemos. Tal como noutros setores da sociedade, também no setor marítimo cada vez mais dependemos da tecnologia para viver como vivemos. Mas julgo que não podemos deixar que seja a tecnologia a determinar como vivemos. São, sem dúvida, as pessoas que devem continuar a contar. E também devem ser as pessoas que devem determinar e marcar a diferença e o caminho.

Regressando ao ponto de partida desta reflexão, voltaria a citar o Professor Dr. António Barreto no âmbito da conferência a que me referi: *O mar é natureza. Por definição, não faz parte do património de um país, entendendo este como essencialmente cultural e técnico. O património é obra humana e resulta da história e da cultura. Mas há realidades naturais que se transformam, pela história, pela cultura e pela técnica, em obras de património. Assim é com o mar para os Portugueses. O mar da pesca, da marinha, das viagens, dos transportes, das praias, do desporto, dos recursos económicos, da fonte de energia, dos civis e dos militares é património. O mar do poema, da literatura, da mitologia, do sonho, dos descobrimentos, da expansão, do império, da Europa e da economia é património e identidade. Há um mar igual ao dos outros, há um mar que é português.* Fim de citação.

Estou convicto de que o valor estratégico do Mar, magnificamente retratado pelo Sr. Professor nestas suas palavras, poderá ser engrandecido através do ciberespaço, se a respetiva segurança estiver sempre presente de forma pragmática e consequente, através de Portugal, na agenda nacional e internacional. Desta forma, enquanto portugueses, estaremos também a reforçar a nosso património e assim a nossa identidade.