# BOLETIM TERTÚLIA

*Encontros e Reflexões*

SEGURANÇA E DEFESA EUROPEIA

VOLUME 1

## PLANO DE RECUPERAÇÃO E RESILIÊNCIA

### OBJETIVOS E DESAFIOS ESTRATÉGICOS

COM O APOIO

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

# Índice

# Editorial

No cumprimento de um dos desígnios da EuroDefense Jovem-Portugal, iniciou-se a 4ª edição das Tertúlias EDJ no passado dia 1 de junho de 2023. Importa destacar duas ideias centrais nesta breve nota introdutória aos artigos desenvolvidos pelos jovens e que compõem este boletim. A primeira ideia refere-se ao papel que a EuroDefense-Portugal, nomeadamente a EuroDefense Jovem-Portugal, tem desempenhado no debate e reflexão sobre as mais diversas áreas das temáticas de segurança e defesa europeia, tendo feito esse papel com especial destaque junto da comunidade jovem. A segunda ideia prende-se com a capacidade de manter esse compromisso com a junção de esforços e empenho por parte de uma equipa de trabalho de reconhecido esforço e mérito. Em especial, destaco todos os que colaboram de forma ativa na organização e execução das iniciativas do nosso Centro de Estudos.

A tertúlias têm-se destacado pela forma pertinente como a comunidade jovem se tem afirmado no processo de diálogo com especialista das mais diversas áreas. Ao longo dos últimos, quando recordamos todas as tertúlias que já foram realizadas pela EuroDefense Jovem-Portugal, desvendamos um diálogo construtivo entre as mais diversas personalidade de elevada relevância e jovens que se afirmam como académicos e profissionais nas áreas debatidas. Esta é uma iniciativa meritória de todo o seu sucesso e cujo o modelo de execução deve ser preservado em benefício de todos os seus intervenientes.

Este boletim concentra um conjunto de desafios que alguns dos nossos jovens procuraram desenvolver sobre a Segurança e Defesa Europeias em Transição. Ao longo dos últimos anos temos assistido a uma crescente incerteza, em matérias desde a cibersegurança, ameaças hibridas, crise de refugiados, economia sustentável, entre muitas outras. Neste boletim vários autores juntaram-se para desenvolver estas temáticas que surgiram no contexto da tertúlia sobre o Plano de Recuperação e Resiliência: objetivos e desafios estratégicos, com a participação do Professor Doutor Nuno Gama Pinto, Vice-Presidente do EuroDefense-Portugal, e abertura do General Luís Valença Pinto, Presidente do EuroDefense-Portugal.

Resta-me desejar ao leitor deste boletim que, em conjunto com a EuroDefense-Portugal, desenvolva uma leitura critica e atenta do futuro da Europa, em especial da sua segurança e defesa.

Com elevada consideração e amizade,
Miguel Carvalho Gomes

# Desafios e Perspetivas da Presença da Huawei na Segurança Cibernética Europeia

Iuri Cláudio, ISCTE – Instituto Universitário de Lisboa

Vitaliy Venislavskyy, Fac. Letras da Universidade de Lisboa

## Resumo

A cibersegurança é crucial para a prosperidade económica da UE, proteção de infraestruturas críticas, preservação da privacidade e dos dados pessoais e defesa contra ciberameaças. Neste sentido, a tomada de decisão de banir todos os serviços de provedoria de rede da empresa chinesa Huawei, o que despoletou um conjunto de tensões entre Bruxelas e a empresa detida pelo Partido Comunista Chinês. Neste paper, são analisadas as consequências geopolíticas desta decisão europeia, caso esta se venha a materializar e também os desafios que a UE enfrenta face a uma implementação de uma Europa Digital, no âmbito do NextGenerationEU.

**Palavras-Chave:** NextGenerationEU; Huawei; 5G; Europa Digital; Cibersegurança

# 1. Introdução

Sob o regime da adoção do Plano de Recuperação e Resiliência Europeu, mais conhecido por Next Generation EU, a União Europeia marcou uma quebra profunda com o anterior modelo de recuperação económica, que se caracterizava por um conjunto de políticas de austeridade (de la Porte, 2021).

Entre outras linhas de ação, a Digitalização tem se tornado num aspeto fundamental para a garantia de segurança em todo o nível europeu, tornando-se, desta forma, numa das prioridades comunitárias para o investimento dos fundos pós-pandemia.

Apesar das enormes divergências observadas durante o processo de negociação, o surgimento, e até o ressurgimento, de várias coligações de atores nestas negociações multilaterais permitiram a União Europeia em ultrapassar os conflitos, mantendo o balanço dos seus interesses, enquanto procuravam concessões e, assim, foi adotado o regime de ajuda financeira para permitir a recuperação europeia do Covid-19 (de la Porte, 2021).

Como de la Porte (2021) identifica, caso o Next Generation EU se torne num instrumento fiscal permanente (cujo potencial, de facto, existe mesmo, devido á projeção do programa), haverá bastantes discordâncias no que toca à sua aplicação nacional, no entanto, a mesma autora refere que o sucesso da aplicação da iniciativa poderá significar a garantia do aprofundamento da integração europeia.

Neste paper, falaremos dos desafios à aplicação das medidas para a digitalização da Europa, sobretudo olhando para o domínio da garantia da cibersegurança, enquanto pilar fundamental para a promoção da segurança social, económica e política da Europa e do mundo. Para tal, será feito um estudo sobre a aplicação destas sanções, por parte dos EUA e a subsequente resposta chinesa. Em segundo lugar, iremos abordar algumas das orientações da UE, para o desenvolvimento do 5G na europa, especialmente pelo facto de poderem vir a afetar influência da Huawei sobre o 5G, visto que as orientações definem algumas caraterísticas constituintes dos atores de risco, e esta empresa pode-se encaixar sobre alguns aspetos. Por fim, faremos uma assessoria sobre as perspetivas futuras destas sanções europeias à China, para o aprofundamento da integração europeia, em matéria digital.

## 2. Desafios à cibersegurança

Em junho de 2023, o Comissário Europeu do Mercado Interno anunciou que a UE está a considerar banir em todos os Estados-Membros os serviços da Huawei, no que consta à provedoria da tecnologia 5G. Estas declarações surgem no sentido de uma recomendação lançada pela Comissão Europeia, ainda em 2020, aos Estados-Membros para que estes diminuam drasticamente a sua dependência da Huawei, na implementação desta tecnologia de rede, devido a fortes suspeitas de que estas expõem inúmeros riscos para a segurança da União Europeia (Laranjeira, 2023).

A discussão do acesso aos dados, por parte dos provedores de redes *online* não é recente, tendo ganho um índole geopolítico de grandes dimensões, aquando do surgimento de conflitualidades entre os Estados Unidos e a China, sobre a provedoria da rede 5G em território norte-americano, resultando na emissão, por parte de Washington, de sanções à China e à Huawei, tais como a proibição à empresa chinesa em prestar serviços de 5G no território dos EUA. Ao mesmo tempo, Washington pressionou a UE para que esta aderisse às sanções e tomasse a mesma decisão.

Pelo contrário, a Comissão Europeia, em 2020, decidiu tratar do assunto através de atos legais não-vinculativos, ou seja, através de recomendações, atribuindo aos Estados-Membros o poder de decisão sobre esta matéria. Desta forma, em quase 2 anos, apenas os Estados do Norte da Europa aplicaram a totalidade das recomendações, expulsando completamente a Huawei, enquanto provedora de serviços de rede *online* 5G (Laranjeira, 2023).

## 3. A relação entre a Huawei e a China

Como referido pela Comissão Europeia em 2021, a segurança das redes 5G é indispensável, dado ao papel importante que podem desempenhar na economia e sociedade europeia, nomeadamente em setores chave como a energia, transportes, banca, saúde e indústria. Portanto, além do 5G ser fundamental em termos de produtividade económica e social, é também uma questão de segurança, já que terá influência em várias áreas críticas da União Europeia (UE).

Uma das principais empresas ligadas ao desenvolvimento do 5G é a Huawei, uma empresa chinesa que tem enfrentado fortes restrições por parte de alguns Estados-

Membros da UE, especialmente pela desconfiança do uso da empresa para fins de espionagem por parte do regime chinês. As preocupações em relação às intenções da China, acrescem quando por exemplo em dezembro de 2018, o FBI anunciou que um grupo conhecido como "APT10" atuou em nome do Ministério da Segurança da China, levando a cabo uma campanha cibernética que visou a invasão a dados comerciais e tecnológicos na Europa, na Ásia e nos Estados Unidos.

Em 2019, os Estados-Membros, com o apoio da Comissão e da Agência da União Europeia para a Cibersegurança (ENISA) publicaram um relatório acerca dos riscos na UE em matéria de cibersegurança relacionada com a rede 5G. Neste relatório, já denotavam riscos, que indiretamente e sem a mencionar a empresa, a Huawei podia apresentar, uma vez que se enquadra em alguns dos critérios necessários para ser considerado como um ator de risco, nomeadamente pelo facto da relação obscura entre a Huawei e o Estado Chinês. É referido que o perfil de risco dos atores aumenta, se existir uma ligação forte entre o fornecedor e o governo do país terceiro, bem como o facto de na legislação não existir controlos e equilíbrios legislativos e democráticos. Desta forma, dada a natureza do sistema político chinês, bem como a legislação em vigor, colocam-se algumas incertezas relativamente aos serviços da Huawei para o desenvolvimento da rede 5G.

Ao nível da relação entre a Huawei e o regime, Tekir (2020), indica que as relações já advêm do passado histórico, pois a empresa foi fundada por Ren Zhengfei, um antigo engenheiro do Exército de Libertação Popular e membro do partido comunista, que detém atualmente 1,14% da empresa. Tekir (2020) refere também que a Huawei foi uma concretização das políticas oficiais chinesas de Deng Xiaoping, nomeadamente o desenvolvimento tecnológico.

Relativamente à legislação em vigor, Hoffman e Kania (2018), destacam que a relação entre os cidadãos e as empresas chinesas estão sujeitas a obrigações legais que colocam em causa a independência da empresa perante o regime. O artigo 7º da Lei dos Serviços Secretos Nacionais, declara que todas as organizações e cidadãos, nos termos da lei, devem cooperar nos trabalhos que envolvam a recolha de informações e manter sigilo sobre os mesmos. As autoras, reforçam ainda o artigo 22º da Lei Contra-Espionagem de 2014 onde é estabelecido que no decurso de uma investigação de contra-espionagem, as organizações e os indivíduos devem fornecer informações verdadeiras e não podem recusar a cooperação. Neste sentido, trata-se de um ambiente legal que potencia o uso das

empresas privadas e respetiva tecnologia como a Huawei, para meios de espionagem do regime chinês (Kaska et al., 2019).

Contudo, a exclusão da Huawei pode vir a ter impactos no desenvolvimento das redes 5G na Europa. A própria Huawei, reconhecendo o seu papel nesta área, solicitou que fosse realizado um estudo acerca dos impactos da exclusão da empresa no desenvolvimento do 5G na europa. De acordo com dados de 2020, dada a posição da Huawei nas contribuições para o 5G as restrições à empresa não só atrasam a implementação desta nova tecnologia, bem como aumentam os custos para os consumidores e empresas (Oxford Economics, 2020). Destaca-se também, num relatório elaborado pelo IPlytics (2021) que a Huawei lidera a corrida às patentes obtidas, comparativamente a outras empresas importantes no mercado global do 5G, como a Nokia e a Ericsson. Destacam ainda, que é a empresa que tem mais influência em termos de contribuições técnicas para o desenvolvimento do 5G.

Assim, apesar da Huawei se enquadrar sobre algumas das caraterísticas que podem potenciar a interpretação desta empresa como um ator de risco do ponto de vista da UE, nomeadamente a possibilidade da Huawei ser um instrumento de espionagem ao serviço do regime chinês, é também uma empresa que não será fácil de evitar na tecnologia 5G devido à importância que detém sobre esta tecnologia, comparando com outras empresas que também se inserem neste mercado.

## 4. Ação política dos EUA – uma visão em retrospetiva

Em termos geopolíticos, hoje observa-se uma ação de "*digital wall*", por parte da China em relação aos EUA, através da qual, a potência oriental pretende criar laços tecnológicos com a UE, tornando-se num meio para a China se tornar no maior Centro Tecnológico Mundial.

Essa ação teve uma resposta rápida, por parte dos EUA, cujo objetivo era de proteger a sua hegemonia e o monopólio de gigantes como a Google e a Apple. Assim, cria-se um problema de desigualdades sociais que pressionam os governos, sendo necessário, deste modo, a delimitação do poder das plataformas digitais estadunidenses (Busquets, 2019).

Desde maio deste ano, que as empresas estadunidenses têm sido proibidas de cooperar com a Huawei, os diplomatas estadunidenses têm tido um grande esforço para influenciar os países, principalmente europeus, para deixarem de usar os produtos da Huawei. Assim,

os EUA procuram, através destas medidas, criar estragos num negócio que eles veem como uma ameaça (The Economist, 2019).

A curto-prazo, trata-se de um sucesso, porque a Huawei chegou a lançar um smartphone sem acesso à Google, nem ao WhatsApp. Somando a isso, vem a reação dos mercados, que mantiveram uma posição de receio face a investimentos nas telecomunicações, enquanto Silicon Valley mostrou um grande susto.

No entanto, Ren Zhengfei (CEO da Huawei) decidiu que ia clonar a tecnologia 5G, na qual o gigante chinês mais investiu, em comparação com o resto do mundo, e vendê-la a uma outra companhia fora da China, defendendo-se desse embargo, mas podendo investir indiretamente na tecnologia 5G. Nesse caso, o mundo estaria dividido em dois ecossistemas tecnológicos, um da Huawei e outro também, mas só em parte. Deste modo, seria criada uma "autoestrada" para uma Guerra Fria, mas desta vez tecnológica (The Economist, 2019).

Fruto dessas sanções americanas, a Huawei tem tido pouco sucesso nas suas vendas. Não só as vendas de telemóveis sofreram quedas, como também as diferentes cooperações nas quais a Huawei participava. Por exemplo, os acordos com a Android para investigações em matéria de software conjunto foram levantados, dado a pressão estadunidense sobre a Google.

Em termos financeiros, a Huawei também perdeu confiança por parte de colossos bancários, como é caso do HSBC e do Standart Chartered (Busquets, 2019).

A venda da tecnologia 5G da Huawei irá levar a muitos riscos, que, caso sejam ultrapassados, darão à Huawei a capacidade de poder envolver novas formas e novas adaptações, tornando-a ainda mais presente nos mercados externos. Deste modo, podendo-se transformar numa empresa de montagem de produtos finais, como também num produtor independente de softwares e hardwares para os próprios dispositivos tecnológicos (Busquets, 2019).

Em suma, assiste-se cada vez mais na cena internacional uma crescente confrontação e procura de soluções por partes destes gigantes tecnológicos num mundo paulatinamente globalizado. Deste modo, é possível destacar pontos transversais ao longo dos artigos e igualmente fatores determinantes na formulação da EPI.

## 5. Conclusão

Em conclusão, apesar da Huawei deter uma grande importância no desenvolvimento do 5G, a UE não está disposta a correr riscos pelas incertezas em torno da relação entre a Huawei e o regime chinês, mesmo que não exista de forma comprovada a relação entre estes dois atores, pelo contrário, a empresa nega todas as acusações, argumentando que é independente de qualquer Governo. Embora, isto não impede que países europeus comecem a aumentar o controlo sobre a empresa de forma indireta.

Por exemplo, em Portugal, a Comissão de Avaliação de Segurança que funciona no âmbito do Conselho Superior de Segurança do Ciberespaço divulgou uma deliberação, em que considerou como "alto risco" a utilização de equipamentos e serviços que, entre os vários critérios, provenham de um "ordenamento jurídico do país em que está domiciliado ou ao qual está, de qualquer outra forma relevante, vinculado, permite que o Governo exerça controlo, interferência ou pressão sobre as suas atividades a operar em países terceiros" (Veríssimo & Nunes, 2023).

No que toca à cena internacional, por sua vez, tem se assistido a uma crescente confrontação e procura de soluções por partes destes gigantes tecnológicos num mundo paulatinamente globalizado. Deste modo, é possível destacar pontos transversais ao longo dos artigos e igualmente fatores determinantes na formulação da EPI.

Aqui destacam-se, em primeiro lugar, a importância da era da digitalização, devido à sua evolução de um desafio a nível económico para um problema político.

Segundo, a dicotomia entre governos e empresas que surge das dificuldades dos governos em se imporem neste processo enquanto autoridade.

Em terceiro lugar, as implicações geopolíticas da estratégia empresarial, que se torna, por exemplo, evidente com a capacidade da Huawei (China) em ascender mundialmente e a vontade dos gigantes estadunidenses em defenderem a sua hegemonia a todo o custo.

Por último, o futuro desafio para as relações económicas internacionais que se observa, resultante do processo de digitalização, leva a criar um grande dilema nas Relações Económicas Internacionais: "Que tipo de liderança ou instituições serão capazes de gerir este enorme desafio?".

É, neste panorama, evidente que a adoção do PRR, sobretudo no âmbito da Reforço do quadro geral de Segurança na base da confiança para a adoção dos serviços eletrónicos, onde, por exemplo, Portugal investe cerca de 47 milhões de euros, poderá dar uma resposta eficiente, já que procura implementar o quadro nacional de cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação. No entanto, esta resposta não é apenas nacional, ela deve ser comunitária, logo deve ser capacitada de uma estrutura legal que a suporte a nível europeu. E a adoção deste enquadramento normativo irá abrir um novo caminho para o reforço da segurança europeia, e, consequentemente, renovar o caminho do aprofundamento da integração europeia.

Para tal, o primeiro passo está em definir, no Tratado da União Europeia ou no Tratado de Funcionamento da União Europeia, o patamar exato em que a Digitalização se encontra, se se trata de um Competência Partilhada, Coordenada ou Exclusiva (quer da UE, quer dos Estados-Membros). E essa definição, por sua vez, leva-nos a refletir sobre a capacidade de resposta que o Tratado de Lisboa confere à União Europeia.

## Bibliografia

Busquets, J.. (2019). Artificial Intelligence And The Challenge Of Global Governance. Forbes. https://www.forbes.com/sites/esade/2019/07/10/artificial-intelligence-and-the-challenge-of-global-governance/?sh=3fc83005636b

European Comission, (2019). Member States publish a report on EU coordinated risk assessment of 5G networks security. Consultado em 12 de maio, 2023. Disponível em https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

European Comission, (2021). The EU toolbox for 5G security. Consultado em 12 de maio, 2023. Disponível em https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

FBI. (2018). APT 10 GROUP. Consultado em 12 de maio, 2023. Disponível em https://www.fbi.gov/wanted/cyber/apt-10-group

Hoffman, S., & Kania, E. (2018). Huawei and the Ambiguity of China's Intelligence and Counter-espionage Laws. The Strategist, 13.

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Center for Excellence (CCDCOE), 28, 1-26.

Laranjeira, F. (2023). UE considera a proibição total obrigatória da Huawei no 5G europeu. Executive Digest - a Leitura Indispensável Para Executivos.

https://executivedigest.sapo.pt/noticias/ue-considera-a-proibicao-total-obrigatoria-da-huawei-no-5g-europeu/

Oxford Economics. (2020). Restricting competition in 5G network equipment throughout Europe. Consultado a 12 de maio, 2023. Disponível em https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/

Pohlmann, T., Buggenhagen, M. (2021). Who leads the 5G patent race November 2021?. IPlytics. https://www.iplytics.com/wp-content/uploads/2021/11/IPlytics-November-2021-Who-leads-the-5G-patent-race.pdf

Tekir, G. (2020). Huawei, 5G network and digital geopolitics. International Journal of Politics and Security, 2(4) (Çin Özel Sayısı)), 113-135.

The Economist. (2019, September 13). Huawei has made a peace offering that deserves consideration. The Economist. https://www.economist.com/leaders/2019/09/12/huawei-has-made-a-peace-offering-that-deserves-consideration

The Economist. (2019b, September 13). Ren Zhengfei may sell Huawei's 5G technology to a Western buyer. The Economist. https://www.economist.com/business/2019/09/12/ren-zhengfei-may-sell-huaweis-5g-technology-to-a-western-buyer

Veríssimo, A., & Nunes, F., (2023). Empresas chinesas banidas da rede 5G. O que está em causa?. ECO. https://eco.sapo.pt/descodificador/empresas-chinesas-banidas-da-rede-5g-o-que-esta-em-causa/01-que-decisao-foi-tomada

# A Legal Vacuum: Cyberspace & EU Normative Doctrine

Ivo Vaz, College of Europe

## Abstract

Scholars and leading EU figures have long assumed that the EU's strength as a World Power is its normative influence. Currently, the two international agreements that attempt at regulating cyberspace are the Council of Europe's Budapest Convention on Cybercrime, and the Shanghai Cooperation Organization's International Information Security Agreement, both however, severely limited in scope and membership. International Law concerning the conduct of war - jus in bello - regulates how wars can be legally fought. The Hague Conventions of 1899 and 1907 and Geneva Conventions of 1949 and 1977 are the most impactful. Nevertheless, disagreement surrounds not only the applicability of existing legal framework for warfare to cyberwarfare, but crucially, whether a new legal framework is even desirable.

In the wake of newly created EU packages, e.g., the Recovery and Resilience Plan, Digital EU, and EU Global Gateway, this paper seeks to address some gaps in strategic thinking, and highlights connection points relevant for the application of these packages.

Importantly, this paper puts forward two questions that need to be addressed in the shortest term possible, namely: in the absence of a generally internationalized will to limit the extent to which cyberspace may be weaponized, is it wise for the EU to keep limiting itself to the label of a Normative Power? And, can Cyber- Security be low-hanging fruit for the communitization of CFSP/CSDP?

**Keywords:** Cyberwarfare; Recovery & Resilience Plan, Digital EU, and EU Global Gateway; Hybrid Threats.

## 1. Introduction

Just as the Industrial Revolution saw the effectiveness of coordinated logistics trough pocket clocks, time-tables and railways (Clausewitz, 1997), the Digital Revolution has weaponized software, information and cyberspace.

The EU finds itself today at a rebranding crossroads. Whereas, after the advents of Brexit, and unpredictability from its US ally, the previous Commission, led by Juncker, did a good job in harnessing unity; after the Covid Pandemic, and the increasingly aggressive stances from the East, the current Commission, led by Von der Leyen, is doing a good job in showing the need for a more proactive and preemptive EU.

With the advancement of policy packages in the form of the Recovery and Resilience Plan, Digital EU, and EU Global Gateway, reasonably expected questions emerge, e.g., What to do with all these packages? Should there be a long-term priority taking precedence over recovery economics? Investing in a greener economy and more microchips are, in themselves, good objectives, but if done as an end rather than as a means to an end, the EU risks playing catch-up politics once again.

This paper will examine how the existing bodies of International Law, State practice, and Doctrines interact regarding Cyber-Warfare; subsequently highlighting the threats the EU faces; and finally, suggesting a reasonable way forward, taking comprehensive advantage of this rebranding crossroads.

## 2. International Law & Cyberspace

The three cornerstone Principles of *Jus in Bello* are the Principles of Distinction, Proportionality, and Unnecessary Suffering. Art. 23 of the Hague Convention projects the Principle of Distinction, limiting attacks to legitimate military objectives, thus prohibiting civilian targets, unless such targets are imperatively demanded by the necessities of war. The Proportionality Principle requires that the use of force in self-defense be limited to that which is necessary to meet an imminent or actual armed attack and must be proportionate to the threat. Attacks on a military objective which cause incidental losses or injury exceeding those needed to obtain concrete and direct military advantage are prohibited (Lewis, 2010). The Unnecessary Suffering Principle prohibits attacks which cannot reasonably be limited to a specific military objective and are indiscriminate in

affecting civilian targets. Thus, the Hague Convention offers examples of such targets as scientific, cultural, or medical infrastructure (Art. 27, HG).

Although no State may claim sovereignty over cyberspace, States may exercise it over cyberinfrastructure within their territory, hence, said cyberinfrastructure is regulated, and such jurisdiction implies both in *personam* and *in rem* (Schmitt, 2013). However, cloud and grid systems may complexify jurisdiction delimitation, thus emerging two doctrines: subjective and objective territorial jurisdiction. Subjective jurisdiction relates to an incident which is initiated within a state's territory but completed elsewhere, applicable even if the offence doesn't affect the territory of the state exercising jurisdiction. Objective jurisdiction grants jurisdiction over individuals to the State where the particular incident has effects even though the act was initiated outside its territory. Other basis for extraterritorial jurisdiction include: nationality of the perpetrator, nationality of the victim, State security, and violation of international law (*id*, 2013).

Nevertheless, the concept of jurisdiction is often mute in context of conflict, hot or cold. Thus, the International Law Commission's Articles on State Responsibility (ASR) have approached the topic of justifiable countermeasures. Accordingly, a State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures (Arts. 22 & 49-53, ASR). Moreover, the ASR impose no requirement for countermeasures to be quantitatively or qualitatively similar to the violation of international law that justified them. Despite this, the Naulilaa arbitral award and the Gabcikovo-Nagymoros judgement, seem to indicate emerging doctrines accounting for the gravity of rights violated. Still, when accounting for Plea of Necessity (Art. 25, ASR) it is not dependent on prior unlawful conduct by another State, but rather imminence of threat or use of force. Additionally, when accounting for Perfidy (Art. 37, Geneva AP1), its prohibition doesn't extend to acts resulting in damage of property, directly implying death or injury to an adversary. Interestingly, the Additional Protocol allows for rouses - acts intended to mislead or induce the reckless enemy conduct - not considered perfidious, since they don't invite confidence, legally allowing endless cyberwarfare possibilities.

The ICJ has stated that articles 2(4) and 51 of the UN Charter apply to any use of force regardless of the weapons employed. Thus, the basic principles of proportionality, distinction, and prohibition of unnecessary suffering are intrinsic in applying the law of armed conflict to cyber operations. Although cyber-operations may not constitute use of

force, they may still violate Article 2(1) of the UN Charter regarding intervention and sovereign equality. The 2007 cyber-attack on Estonia did not arouse the application of the law of armed conflict because it did not escalate to war. Cyber-attacks rarely release physical impact, yet can cause great injury to people and objects, *e.g.,* electric grids, communication systems, nuclear facilities, hospitals, *etc*. (Schmitt, 2013).

## 3. Cyber Doctrines & Foreign Policy

In cyberspace states engage in acts short of war. Whilst International Law and world leaders remain divided on approaches, technology has allowed a cyber arms race. This weaponization of cyberspace opened at least two basic approaches: active and passive engagement. Active Engagement sees cyberspace as essential for modern warfare: operationally, since soldiers are increasingly dependent on cyberspace; and strategically, both in deterrence and exploitation of weaknesses. Cyberspace dynamics make it is easier to attack than to defend, thus encouraging offence (Hjortdal, 2011). There are three main Computer Network Operations (CNO): Computer-Network Exploitation (CNE), gathering information for later attacks; Computer-Network Attacks (CNA), attacking systems; and, Computer-Network Defense (CND), defense mechanisms. Effective CNA cannot be carried out without also CNE and CND and vice-versa (*id*., 2011). Incentives for an aggressive cyber-posture are threefold: to deter other states by infiltrating their critical infrastructure; espionage for faster military development; and, industrial espionage for economic gains (*id*, 2011). Whereas Active Engagement is interpreted as spiraling into Realism's "security dilemma", Passive Engagement refuses to play a tit-for-tat game, instead silently collecting information from the cyberattacks. By restraining oneself, one becomes aware of one's own vulnerabilities, and thus more capable of creating Punji traps, akin to cyber guerrilla warfare (Burk & Kallberg, 2016).

China developed its cyberwarfare capabilities in the early 2000s with spear-phishing - which is still a staple of Chinese cyber-tactics. Beijing subsequently spread hacker units across its apparatus (PLA, Ministry of State Security, *etc*.) (Buchanan, 2020). China launched such an aggressive initial campaign for a reason: it lacks the home-field advantage that the Five Eyes enjoy. Beijing is far less optimally placed on the world's data flows and its technology companies do not command the world's data in the way that GAFA does – despite having currently mitigated said disparity in the 5G race. Passive

collection and corporate access serve the regime well within its borders, but if the government seeks greater awareness beyond the *Great Firewall*, it must hack targets proactively. Spear-phishing is often the easiest way in (id., 2020). China's military strategists describe cyber capabilities – specifically CNAs - as a powerful asymmetric tool for deterrence, at minimum by increasing the enemy's costs of engagement in the first place, characterizing CNAs as a preemptive weapon (Hjortdal, 2011).

Many cyber-analysts now consider China as the most extensive and aggressive world power regarding cyber-engagement, highlighting the infiltration of more than 100 countries' networks to track exiled Tibetans (Glaister, 2009). Indeed, MI5 has reported that any UK company is at risk if it holds information beneficial to Beijing, further detailing how China's cyber-warfare campaign targets British defense, energy, communications and manufacture companies, as well as law firms (Corera, 2022). The FBI has also reported on a Chinese cyber army of almost 200 thousand spies from both the military and private sector. The British Joint Intelligence Committee, which coordinates work between MI5 and MI6, has also warned about Chinese cyber exercises designed to shut down critical UK services e.g., energy, agriculture, and water supplies (Hjortdal, 2011).

Though Europe has been accustomed to "Eastern-coming" threats, it seems to have failed to acknowledge a Sino-Soviet rapprochement, cyber-specifically speaking. This alignment extends far beyond a regional *ménagement* in central Asia (Lubina, 2017). Europe has preferred to outsource its status as a military power to the US, labeling itself as a normative power, setting realist doctrines aside, and focusing on liberal institutionalism (Vaz, 2023).

Europe has not, however, considered the possibility of being overtaken as a normative power by unsuspecting powers. Today's Sino-Russian normative partnership poses key challenges, putting the liberal foundations of multilateral institutions to the test (Ekman, 2020). China and other emerging great powers do not want to contest the principles of the liberal international order, they wish to gain more authority and leadership within it (Ikenberry, 2011). Beijing and Moscow in particular challenge the normative values promoted by the EU employing tactics of propaganda, disinformation, and manipulation (Ekman, 2020).

China and Russia's policy coordination and collaboration in International Law have become pronounced (Averre & Davies, 2015). As highlighted by a joint declaration, in 2016 (PRC MFA, 2016), underscoring the sides will to further enhance their cooperation in upholding and promoting international law and establishing a just and equitable international order. Cyber-governance is a clear area of Sino-Russian convergence dating to the 2000s, when they set up a bilateral intergovernmental sub-commission on communication and information technology, with a regional code for cyber-behavior under the SCO (Ekman, 2020), and even a bilateral treaty for policing illegal online content (SCMP. 2019). Moscow and Beijing have thus striven to shape the cybersecurity narrative under a label of "information security", even taking precedence over security of cyber infrastructure (Art. 2 SCO Treaty).

Normatively they have been effective, as evidenced in 2019 by a joint Sino-Russian effort securing a UN resolution (Peters, 2019), posing an alternative to the Budapest Convention, which would impede the gathering of cyber evidence in criminal cases (Ekman, 2020). It's worth remembering that even before Russia was ousted from the Council of Europe (Gotev, 2022), it was the only member-state to not have signed the Budapest Convention, under which parties collaborate towards investigation and collection of evidence of any electronic form of criminal offence (Art. 23, Budapest Convention) - allowing parties to access OS data, regardless of where it's geographically located, without third party authorization. Finding this to infringe State sovereignty, Moscow and Beijing have established their own cyber convention under the SCO (Pierri, 2018), and continue their normative push today (Page, 2022).

## 4. Hybrid Warfare

The Sino-Russian partnership highlights digital power projection. The USSR had developed a doctrine known as "*Maskirovka*" (Roberts, 2015). It supported the creation of illusions through concealment, simulation, diversion and disinformation. In today's geopolitical arena it is better known as Hybrid Warfare (Stenslie, 2021). These amorphous sets of threats exist at levels short of war, enabling powers to exploit societal divisions and instigate instability in democratic systems – *a.k.a., Psy-Ops*. The EU, as it stands today, is a playground for Hybrid Warfare (Gressel, 2019).

not the most materially damaging use of cyber capabilities (Webber & Yip, 2018), hybrid threats are extensive intelligence, conspiratorial, and subversive efforts used to weaken an opponent's society through employment of fake news, information warfare, social media manipulation, and hacktivism (Schnaufer, 2017) - thus being the optimal stealth tactic in cyber warfare.

On EU soil, the MacronLeaks (Matishak, 2017) offer a pertinent example of Russian hybrid warfare. Given that the campaign is regarded as a failure (Vilmer, 2019), it serves as useful reflection over the French Cyber Doctrine. Though subtle in action (Wallace, 2019), France is a long-standing CyberDefense power in the world, boasting both offensive and defensive capabilities (D'Elia, 2018).

Recently however, France has been more upfront about its cyber capabilities. In 2016 France announced the established a Cyber Command composed of almost 3000 cyber-fighters (Delerue, & Géry, 2018). Indeed, France's Defense Ministry publicly remarked that MacronLeaks was an afront to French democratic foundations, highlighting France's right to retaliate not only through its cyber arsenal, but by conventional armed means as well (Conley & Vilmer, 2018).

Attesting for French competence countering the MacronLeaks, the Macron campaign enacted honeypots, false flags and forged documents under the pretense that they would be hacked, thereby inundating, confusing and slowing the attackers (Gallagher, 2017). Marcon's team communicated openly and extensively about the hacking and disinformation operations, thus gaining control over the leaked information (Faesen, 2020). Benefiting from the lack of an effective transmission belt (Gressel, 2019), Macron focused more on the combination of preventive cyber resilience and active debunking of disinformation than offensive engagement (Dearden, 2017).

While Chinese hybrid operations are less visible than Moscow's, Beijing is very active, seeing Europe as a softer target than the US. It concentrates on launching skilled cyber-attacks against industries and research facilities (Gressel, 2019). Additionally, the sovereign dept crisis became the perfect opportunity for exploiting member-state divisions, facilitating Chinese dept diplomacy not only in economically weaker member-states, but also EU aspiring Balkan States (Meunier, 2014).

Europe's increased vulnerability to hybrid attacks inherently linked to technological progress and globalization (Smit, 2022). Europe's political elite developed a Fukuyaman

view, neglecting its harsh global and regional reality. The wars in Ukraine and Syria have dented in this world view (Guriev, 2023).

Consequently, when confronted with geopolitical pressure, i.e., hybrid threats or hyper-aggressive intelligence action, European governments' first instinct is of patient engagement. Increasingly, adhocism marks institutional progress, hampering a more coordinated EU-level response (Vaz, 2023). This is especially the case on the most threatening hybrid attacks, e.g., the diplomatic expulsions following the Skripal affair (Haines, 2018), which took place outside the EU framework; and the Russian attack on the Organization for the Prohibition of Chemical Weapons (Dettmer, 2018). When this became public, non-EU member-states released more forceful support statements than those from EU member-states, even though OPCW headquarters are in EU territory (Gressel, 2019).

## 5. A Way Forward

EU cyber-diplomacy and cyber-defense must become more ambitious in developing diplomatic structures resilient against hybrid, cyber, and intelligence risks, thus fostering cyber alliances aimed at capacity-building, cybersecurity strategies and standards.

In so doing, it would prove efficient to act within pre-existing channels (Keukeleire & Delreux, 2014), aiming not for more points of contact, but toward solidification and consistency of existing strategic partnerships, particularly in Asia (Banim, 2017). However inconsistent the UK was concerning EU defense integration, the EU effectively lost whatever foot it had vis-à-vis the 5 Eyes with Brexit (Saleem, 2019). Nevertheless, there is untapped potential not only for furthering EU security integration, but also aggregating the potential in the Far-East States outside the 5 Eyes (Janning & Möller, 2019). External Action cyberpolicy may be low-hanging fruit (KUL, 2021).

South Korea is consistently among the top ten destinations of EU arms exports. The EU's share of Seul's total arms imports doubled between 2013-2017 and the previous five-year period. This is due to South Korea diversifying its arms import through significant reductions of US arms exports. Even if the US will likely remain Seul's kenetic security guarantor, frustrations with Washington have opened up South Korea's defense market

for Europe. This is most evident in the case of munitions and missiles (Stanley-Lockman, 2018).

Until recently, the Japanese Constitution prohibited defense industrial cooperation with foreign partners (Schneider, 2012). Japan began easing restrictions on arms exports in 2011 (Schlesinger & Nakamichi, 2011), culminating in lifting the ban in 2014 to proactively contribute to peace in the region (Takenaka, 2014). 2017 was pivotal for bilateral defence relations between Japan and EU member-states. France, Germany, Italy, Sweden and the UK signed agreements regarding defense technology cooperation with Tokyo. Aimed at signaling Tokyo's goal to diversify its defense network with partners beyond Washington, in aggregate, these events could constitute a framework for military partnerships with the EU (Stanley-Lockman, 2018).

The Indo-French strategic partnerships lay outside Europe and NATO. Launched in 1998 under Jacques Chirac, one year after the establishment of the global partnership with China. Defense and military cooperation, stands as a central area of cooperation, involving politico-military dialogues, armament transfers and joint exercises (Saint-Mézard, 2015).

Taiwan's government faces 20 to 40 million cyberattacks every month, according to their Director General of the Cyber Security. Taiwan's National Security Bureau alone faces roughly 100,000 hacking attempts every month. In 2017, Taiwan's Department of Cyber Security reported 360 successful attacks on government systems, 288 of these launched by Chinese network forces. The attacks mostly have been categorized as Advanced Persistent Threats and Active State Sponsored Malware Campaigns (Pryor, 2019). As such, there is much to be learned from Taiwan. In response to its military being frequently targeted, Taiwan created a cyberwarfare branch as the fourth branch of its armed forces (Weber, 2022) - the first such independent military cyber command in the world (Fahey, 2018).

Finally, ASEAN represents the EU's third-largest trading partner after the US and China, while the EU has tended to be South-East Asia's greatest FDI source. However, ASEAN has so far refused to grant the EU membership in the key ASEAN-led regional multilateral security organization (ADMM-Plus) (Heiduk & Wong, 2021). This is due to Security and Defense integration within ASEAN member-states being slow and tedious (Wong & Brown, 2016). However, cyber-security, might be low-hanging fruit both for EU-ASEAN

and intra-ASEAN integration, given its novelty regarding military and defense (Christiansen, 2021).

## 6. Conclusion

This paper briefly outlined the applicability of international law to Cyberwarfare, seeing it above all as a difficult endeavor. First, since attribution is complex in both in practical and political terms; secondly, since the lack of enforcement and the permissibility of countermeasures are mutually enforcing factors; thirdly, since perfidy is rendered by legitimate employment of rouses and espionage; and, finally, since there is a very specific definition of what constitutes war and armed conflict, Cyberwarfare sits on an obtuse line of actions short of war. By extension of reasoning, it is quite improbable that the powers at play would spontaneously agree to limit their own asymmetric arsenal by way of an overarching convention on Cyberwarfare, and even if they did, at the current pace of technological development, it would be a colossal feat of Law.

This paper thus argues in favor of an EU Cyberwarfare doctrine more akin to Active Engagement, not only because cyberspace in a dual-use realm wherein integration would not *per se* infringe upon CFSP intergovernmentalism; but crucially because being passively on the receiving end can prove to be at best exhaustive and at worst putting one's own vitality at risk *e.g.,* election interference – the cases of Estonia, Ukraine, Hong Kong and Taiwan are cases in point. Through Active Engagement one can at least force the enemy to divert part of its resources away from all-out offensive action, and in doing so perfect policy and aggregate experience, and capabilities further up the learning curve.

EU bureaucracy and *adhocism* simply spreads its capabilities too thin. Something made worse by having overrated its focus on civil power and normative influence. While allying with the USA may have been, and to arguable extent still is, a positive decision, it has depreciated its autonomy and decisiveness. Illusioned by the end of the Cold War, Europe finds itself at a turning point, never has it been easier to divide and conquer. This paper argues in favor of a more proactive stance, specifically playing a "geopolitical Uno reverse card", turning East to foster friendly cooperation with States that not only fall victim to similar threats but that are also more used to them due to geographical proximity.

Moving forward the EU should definitely take advantage of DigitalEU. DigitalEU is just as much about cyber security as it is about consolidating the EU internal market, strengthening Foreign Policy instruments, and projecting EU innovation & technology capabilities. Some proposals are *Gaia-X*, the *Digital Services Act*, the *Data Governance Act*, and the *Chips Act* – all of which would prove decisive both in geopolitical and geoeconomical terms for the pursuit of the above-mentioned Uno reverse card, fitting perfectly within the ambitions of the EU Global Gateway which aims to rival China's BRI.

## References

Averre, D. & Davies, L. (2015) Russia, Humanitarian Intervention and Responsibility to Protect: the case of Syria. International Affairs.

Banim, G. *et al* (2017) Prevention better than cure: the EU's quiet diplomacy in Asia. European Institute for Security Studies.

Buchanan, B. (2020) The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Burk, R. & Kallberg, J. (2016) Bring on the Cyber Attacks. Army Cyber Institute.

Christiansen, T. (2021) Security Relations with Asian Partners. Palgrave Macmillan.

Clausewitz, C. (1997) On War [J. J. Graham, Trans.]. Wordsworth Editions.

Conley, H. & Vilmer, J. (2018) Successfully Countering Russian Electoral Interference. Center for Strategic & International Studies.

Corera, G. (2022) China: MI5 and FBI heads warn of 'immense' threat. BBC.

Dearden, L. (2017) Emmanuel Macron hacked emails: French media ordered by electoral commission not to publish content of messages. The Independent.

Delerue, F. & Géry, A. (2018) The French Strategic Review of Cyber Defense. Italian Institute for International Political Studies.

D'Elia, D. (2018) Industrial policy: the holy grail of French cybersecurity strategy? Journal of Cyber Policy.

Dettmer, J. (2018) How a Blunder Unmasked 305 Russian GRU Agents. VoaNews.

Ekman, A. *et al* (2020) The Sino-Russian Normative Partnership in Action. European Union Institute for Security Studies.

Faesen, L. (2020) Case Studies of Norm Development in Hybrid Conflict. Hague Centre for Strategic Studies.

Fahey, M. (2018) Taiwan enacts Cyber Security Management Act. Winkler Partners.

Gallagher, S. (2017) Macron campaign team used honeypot accounts to fake out Fancy Bear. ArsTechnica.

Glaister, D. (2009) China accused over global computer spy ring. The Guardian.

Gotev, G. (2022) Russia leaves Council of Europe, avoiding being kicked out. Euractive.

Gressel, G. (2019) Protecting Europe from Hybrid Threats. European Council on Foreign Relations.

Guriev, S. (2023) The Return of The End of History. The Japan Times.

Haines, J. (2018) Moscow Rules: The Skripal Affair. Foreign Policy Research Institute.

Heiduk, F. & Wong, R. (2021) Security Relations Between the EU and Asian. Palgrave Macmillan.

Hjortdal, M. (2011) China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. University of Copenhagen Centre for Military Studies.

Ikenberry, J. (2011) The Future of the Liberal World Order: Internationalism After America. Council on Foreign Relations.

Janning, J. & Möller, A. (2019) Untapped potential: How new alliances can strengthen the EU. European Council on Foreign Relations.

Keukeleire, S. & Delreux, T. (2014) The Foreign Policy of the European Union. Palgrave Macmillan.

LeuvenGGS (09/06/21) Revisiting Decision-Making in the EU's CFSP: Time to Act? [Video] YouTube.

Lewis, J. (2010) A Note on the Laws of War in Cyberspace. Center for Strategic & International Studies.

Lubina, M. (2017). Central Asia: Towards Sino-Russian Condominium. Verlag Barbara Budrich.

Matishak, M (2017) NSA chief: U.S. warned France about Russian hacks before Macron leak. Politico.

Meunier, S. (2014) A Faustian bargain or just a good bargain? Chinese foreign direct investment and politics in Europe. Asia Europe Journal.

Nabeel, F. (2019) International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. Centre for Strategic and Contemporary Research.

Page, M. (2022) The hypocrisy of Russia's push for a new global cybercrime treaty. The Lowy Institute.

Peters, A. (2019) Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime. Foreign Policy.

Pierri, B. (2018) Cyber Security and Cyber Crime: A Comparative Study in a New "Cold War" Scenario. Eunomia. Rivista semestrale di Storia e Politica Internazionali.

Pryor, C. (2019) Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership. Center for Strategic and International Studies.

Roberts, J. (2015) Maskirovka 2.0: Hybrid Threat, Hybrid Response. Center for Special Operations Studies and Research.

N. (2007) War Crimes from Cyberweapons. Center for Information Security Research U.S. Naval Postgraduate School.

Saint-Mézard, I. (2015) The French Strategy in the Indian Ocean and the Potential for Indo-French Cooperation. S. Rajaratnam School of International Studies.

Saleem, M (2019) Brexit Impact on Cyber Security of United Kingdom. Queen Mary University of London.

Schlesinger, J. & Nakamichi, T. (2011) Japan Moves Toward Easing Military Exports Ban. The Wall Street Journal.

Schmitt, M. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Schnaufer, T. (2017) Redefining Hybrid Warfare: Russia's Non-linear War against the West. Journal of Srategic Security.

Schneider, G. (2012) The Political Economy of Arms Export Restrictions: The Case of Japan. Japanese Journal of Political Science.

SCMP (2019) China and Russia to sign treaty aimed at combating illegal internet content. South China Morning Post.

Smit, S. et al (2022) Securing Europe's Competitiveness: Addressing its technology gap. McKinsey Global Institute.

Stanley-Lockman, Z. (2018) Europe-Northeast Asia defence relations: heralding a new era. European Union Institute for Security Studies.

Stenslie, S. et al (2021) Intelligence Analysis in the Digital Age. Routledge.

Takenaka, K. (2014) Japan relaxes arms export regime to fortify defence. Reuters.

The Charter of the United Nations. San Francisco. 26/06/1945.

The Declaration of the People's Republic of China and the Russian Federation on the Promotion of International Law. Beijing. 25/06/2016.

The International Law Commission's Articles on State Responsibility. In *Annex to General Assembly Resolution 56/83.* UN. 12/12/2001

The Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague. 18/10/1907.

The Protocols additional to the Geneva Conventions. Geneva. 12/08/1949.

The Shanghai Cooperation Organization Treaty. Beijing. 15/07/2001.

Vaz, I. (2023) EU Law in Foreign Security and Defense Policy: Administration and Leadership from the High Representative's Perspective. NOVA University Press.

Vilmer, J. (2019) The "Macron Leaks" Operation: A Post-Mortem. Institut de Recherche Stratégique de L'École Militaire.

Wallace, D. et al (2019) Peeling Back the Onion of Cyber Espionage after Tallinn 2.0. Maryland Law Review.

Webber, C. & Yip, M. (2018) The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. International Journal of Cyber Criminology.

Weber, V. (2022) Taiwan's Offensive Cyber Capabilities and Ramifications for a Taiwan-China Conflict. Council on Foreign Relations.

Wong, R., & Brown, S. (2016). Stepping up EU-ASEAN Cooperation in Non-Traditional Security. *In Changing Waters: Towards a New EU Asia Strategy*. LSE Ideas Special Report.

Wong, R. & Heiduk, F. (2021) Security Relations Between the EU and ASEAN. In *The European Union's Security Relations with Asian Partners*. Palgrave Macmillan.

# Migração na União Europeia: Um Olhar Abrangente sobre Desafios e Políticas

Jorge Silva, Universidade Católica Portuguesa – Lisboa

Vitaliy Venislavskyy, Fac. Letras da Universidade de Lisboa

## Resumo

Desde o estabelecimento da União Europeia, esta tornou-se num destino, por excelência, dos principais fluxos de migração, que originam sobretudo da periferia da EU. Neste artigo, é examinada a migração forçada com destino à União Europeia, tendo em conta o seu enquadramento normativo. Da mesma forma, são analisados dois principais objetivos destes fluxos, o de 2015, vindo do Norte de África e do Médio Oriente, tal como o de 2022, vindo da Ucrânia. Assim, são analisadas as fragilidades da reação europeia, enquanto se observa os planos do NextGenerationEU em resolver estes desafios, a nível comunitário.

**Palavras-Chave**: NextGenerationEU; Migração; Ucrânia; Refugiados; Médio Oriente

## 1. A migração forçada e o Direito Internacional Humanitário

O afluxo de milhões de pessoas causado pela guerra é um dos maiores desafios humanitários. Quando as pessoas são forçadas a abandonar as suas casas e a sua vida, a saúde física e mental é afetada. Podem perder a sua independência, sentir-se inseguras, não conseguirem acesso a serviços essenciais e exporem-se a perigos sanitários e a episódios de violência. As migrações têm um peso muito significativo no país hospedeiro, em particular se esse país tiver falta de meios e apoios necessários. (ICRC, 2019).

Quando nos referimos a pessoas deslocadas em consequência de um conflito armado, o Direito Internacional Humanitário (DIH) deve fazer parte integral da reflexão em como reduzir e resolver o problema das migrações durante um conflito armado, inclusive para responder à questão se a violação do DIH tem o efeito de aumentar ou diminuir o número de pessoas deslocadas. (ICRC, 2019)

Os migrantes que fogem de um conflito não são vítimas passivas, mas verdadeiros participantes ativos. Apesar de forçados a tomar uma decisão, são as pessoas que escolhem entre ficar ou fugir, e para onde se deslocar. Por vezes essa escolha é feita de forma instantânea, mas existe ocasiões em que a escolha é ponderada e tomada de forma racional com os restantes familiares, tendo em conta o risco que permanecer representa e se têm os recursos necessários para a mudança. (ICRC, 2019)

A principal causa do afluxo migratório é a violência: as evidências demonstram que existe uma correlação direta entre o aumento da violência e o aumento de pessoas deslocadas. O conflito é, por natureza, violento.

Enquanto os atos de violência que atingem civis podem constituir violações do Direito Internacional Humanitário, existem diversos crimes que, direta ou indiretamente, potenciam as migrações, nomeadamente: violação dos princípios e regras que regulam os conflitos; uso ilegal de minas antipessoais; ataque direto a infraestruturas civis e instalações para o fornecimento de serviços básicos e a disrupção destes serviços; entre outros.

O termo “pessoas deslocadas” é definido como: “Pessoa que abandona o seu Estado ou a sua comunidade por ter medo ou por correr perigos diferentes daqueles que lhe confeririam o estatuto de refugiado. Uma pessoa deslocada é, com frequência, forçada a

fugir devido a conflitos internos ou a desastres ambientais, naturais ou provocados pelo Homem” .

Migração forçada “é usado para caracterizar o movimento migratório em que existe um elemento de coação, nomeadamente ameaças à vida ou à sobrevivência, quer tenham origem em causas naturais, quer em causas provocadas pelo homem (por ex., movimentos de refugiados e pessoas internamente deslocadas), bem como pessoas deslocadas devido a desastres naturais ou ambientais, químicos ou nucleares, fome ou projetos de desenvolvimento” . Nos termos do DIH é proibido, às partes conflituantes, forçar a migração de civis, exceto se a segurança dos respetivos civis ou razões militares imperativas assim o exijam.

O DIH, no entanto, não tem como objetivo parar ou proibir determinadas formas de violência, mas sim limitar o sofrimento que a guerra provoca, criando um equilíbrio entre a prioridade humanitária e a necessidade militar. O mesmo se aplica às migrações - os conflitos armados são sempre violentos, e provocam migrações forçadas e obrigam civis a fugir, mesmo que ambas as partes estejam abrangidas pelas normas do DIH. (ICRC, 2019).

As migrações são parte da guerra. Existe um elemento que surge sempre, quando e onde existe um conflito. Esse elemento é a violência, seja em violação do DIH ou não. As evidências demonstram que existem mais pessoas a migrar em consequência da violência do que por outra causa. A violência ainda é a principal causa do fluxo migratório.

## 2. O que diz o Direito Internacional sobre migração forçada

Não existe uma definição universalmente aceite de “migrante” e a decisão de migrar pode ser voluntária ou forçada. Factos como conflitos armados ou desastres naturais, podem ser a razão principal e imediata que obriga os civis a fugir de casa. A busca de melhores oportunidades económicas, as alterações do meio ambiente, a crescente repressão dos direitos e a disponibilidade de redes familiares em locais mais estáveis podem determinar com precisão para onde os migrantes se deslocam e por quanto tempo. Também se denomina de “migração heterogénea” para descrever a condição das pessoas que fogem de conflitos armados em busca de asilo, refugiados e pessoas apátridas. (ICRC, 2015)

Nos conflitos armados internacionais, o Art49(1) da IV Convenção de Genebra proíbe "as transferências forçadas, em massa ou individuais, bem como as deportações de pessoas protegidas do território ocupado para o da Potência ocupante ou para o de qualquer outro país, ocupado ou não... qualquer que seja o motivo". No entanto, a Convenção não impõe uma proibição total – no segundo parágrafo do mesmo artigo podemos ler que: "Contudo, a Potência ocupante poderá proceder á evacuação total ou parcial de uma dada região ocupada, se a segurança da população ou imperiosas razões militares o exigirem" (Art. 49 da IV Convenção de Genebra).

O art. 17º do Protocolo II Adicional às Convenções de Genebra estipula que "a deslocação da população civil não poderá ser ordenada por razões relacionadas com o conflito, salvo nos casos em que a segurança das pessoas civis ou razões militares imperativas o exijam..." No segundo parágrafo do mesmo artigo está escrito que "As pessoas não poderão ser forçadas a deixar o seu próprio território por razões que se relacionem com o conflito" (Art. 17º do Protocolo II Adicional às Convenções de Genebra).

No entanto, não devemos negligenciar o facto de que o deslocamento de pessoas é mais do que apenas uma consequência da guerra, ou o resultado de violações do DIH. Em alguns casos pode ser uma estratégia deliberada. Quando analisamos o que provoca a fuga das pessoas devemos avaliar as ações que obrigam a população a migrar. Por vezes as partes de um conflito recorrem a métodos encobertos, tais como migração forçada, coagindo as pessoas a deixar as suas casas ou transferindo-as à força. As partes conflituantes nunca mencionam explicitamente a ordem para deslocar, nem organizam essa mesma transferência, mas provocam de forma deliberada através de ataques diretos a civis, violência sexual, ameaças contra a vida das pessoas e a sua segurança e ataques diretos contra os bens das pessoas (ICRC, 2019).

## 3. Ucrânia – a migração em curso

Na Ucrânia, uma onda de migrações foi despoletada pela invasão ilegítima da Rússia no Leste do país. A situação da Ucrânia demonstra uma correlação direta entre a violência provocada pelos conflitos armados e o aumento de pessoas deslocadas. (ICRC, 2015).

Desde que a Rússia lançou a ofensiva militar contra a Ucrânia a 24 de fevereiro de 2022, os civis foram envolvidos num fogo cruzado. Áreas residenciais, hospitais e escolas são

ameaçados. O conflito desencadeou a maior vaga de migração em décadas. Enquanto a guerra aumenta de intensidade e os civis enfrentam a escassez de água, comida e medicamentos, o número de refugiados à procura de proteção aumenta a cada dia nas fronteiras internacionais. Estima-se que pelos menos 6,5 milhões de pessoas tenham sido deslocadas internamente na Ucrânia, de acordo com dados do Cluster de Proteção das Nações Unidas. (Parrish, Filo)

A maioria das pessoas deslocadas internamente procuram refúgio junto das respetivas famílias, amigos ou em alojamentos arrendados em caves ou garagens subterrâneas. O custo do arrendamento, em particular na zona ocidental da Ucrânia, aumentou exponencialmente devido à elevada procura. Inúmeras pessoas estão a deslocar-se para abrigos coletivos, tais como edifícios públicos, onde podemos incluir escolas, igrejas, ginásios e teatros, onde a falta de divisão entre géneros aumenta o risco de violência de género. Apesar de estarem a ser reunidas melhores condições para enfrentar estas e outras dificuldades, a verdade é que é necessário mais apoio para resolvê-los de forma definitiva. (Parrish, Filo)

Existem evidências claras de que tem existido deslocações forçadas de menores para o território ocupado pela Rússia, ou para o interior da Federação Russa. Existe um sentimento de preocupação de que as autoridades russas estejam a adotar um procedimento simplificado para conceder a cidadania russa a crianças órfãs ou que não estejam acompanhadas pelos respetivos pais. Nos termos do Art. 50 da IV Convenção de Genebra, a Federação Russa está proibida de alterar os dados pessoais destas crianças, incluindo a sua nacionalidade. Adicionalmente, as autoridades russas estão a permitir a deslocação de crianças da Ucrânia para famílias na Federação Russa sem que exista o pressuposto de reunião familiar, ou qualquer respeito pelo superior interesse da criança. (Kehris, 2022).

Adicionalmente, as Forças Armadas Russas têm submetido os civis á denominada "filtragem", um procedimento de segurança onde é realizada uma revista completa ao civil, e a recolha exaustiva dos seus dados pessoais. As pessoas sujeitas à "filtragem" inclui aquelas que estão a abandonar as zonas de conflito, e os residentes ou os que se encontrem em movimento nos territórios controlados pela Federação Russa. Apesar dos postos de controlo de segurança não serem proibidos nos termos do Direito Internacional Humanitário, existe preocupação relativamente a estes procedimentos, e as detenções que lhes seguem, não respeitando os princípios da necessidade e da proporcionalidade. Este

procedimento já resultou em enumeras violações dos direitos humanos, incluindo o direito á liberdade, segurança e privacidade. As Forças Armadas Russas, durante as inspeções, já sujeitaram pessoas a revistas corporais, interrogatórios intensivos sobre a história pessoal, ligações familiares e a opinião política. Também analisaram os bens pessoais, incluindo o acesso aos respetivos telemóveis e informação privada, imagens e impressões digitais. Existe uma particular preocupação relativamente às mulheres e meninas que estão perigosamente sujeitas ao risco de violência sexual durante estes procedimentos. (Kehris, 2022).

Nas primeiras cinco semanas do conflito, mais de quatro milhões de ucranianos procuraram proteção nos países vizinhos, e mais 6,5 milhões de pessoas foram obrigadas a deslocarem-se internamente, tornando esta na maior migração das últimas décadas. Enquanto a intensidade do conflito aumenta e os bens essenciais incluindo comida, água e medicamentos escasseiam, o número de refugiados continua a aumentar. Os países mais próximos da Ucrânia, em particular a UE, têm adotado políticas que facilitam a migração de refugiados ucranianos, a maioria sendo mulheres, crianças e idosos. Em particular, as pessoas com deficiências e os mais idosos têm tido muitas dificuldades em alcançar proteção, muitas vezes devido á sua dificuldade de movimentação. (V. Rabus, 2022)

Para além dos 6.5 milhões de pessoas deslocadas internamente, estima-se que 12 milhões de pessoas se encontrem impedidas de sair das zonas afetadas, sem capacidade ou vontade de deixar as suas casas para trás. A destruição das ligações ferroviárias e rodoviárias, e até a falta de informação sobre as opções que os civis dispõem, está a dificultar a sua evacuação. Estas pessoas são as mais vulneráveis porque estão diretamente expostas aos ataques e completamente impossibilitadas de receber água, comida e medicamentos. (Parrish, Filo, 2022)

Com as hostilidades em curso, existem vários cenários que podem acontecer. Até agora, muitas das pessoas que migraram têm sido da região leste do país para a zona central ou ocidental da Ucrânia. Dependendo do que acontecer no Leste, norte ou sul, podemos antecipar mais movimentações entre estas regiões ou para o ocidente. A Organização Internacional para as Migrações (IOM) concluiu que 26 por cento das pessoas deslocadas internamente no Leste ucraniano, 20 por cento no Sul e 19 por cento no ocidente têm intenções de continuar a sair para outro lugar, no entanto apenas 12 por cento na Ucrânia central e 10 por cento no Norte fazem a mesma afirmação. (Parrish, Filo, 2022)

Dado estarmos perante uma situação extremamente volátil, não é possível estimar quantas pessoas ainda permanecerão deslocadas dentro da Ucrânia, e quantas irão procurar proteção noutras fronteiras internacionais. A insegurança combinada com a destruição dos casas e infraestruturas, significa que as pessoas irão permanecer deslocadas durante um período de tempo alargado. Adicionalmente, a falta de comida, médicos, eletricidade, gás e água ainda agrava a atual situação na Ucrânia para aqueles que se encontram em fuga. (Parrish, Filo, 2022)

O impacto socioeconómico do conflito ameaça reverter décadas de desenvolvimento e de luta contra a pobreza. A UNDP (United Nations Development Program) estima que as condições piorem. 90 por cento da população ucraniana poderá enfrentar a pobreza e dificuldades económicas severas. De acordo com o Ministério da Economia, a Ucrânia sofreu perdas e danos no valor de quase 565 biliões de dólares americanos desde 24 de fevereiro de 2022.

## 4. Os fluxos migratórios na UE

A atual narrativa política europeia procura uma abordagem holística e de longo à resolução dos desafios que se colocam com os crescentes fluxos migratórios com destino à União Europeia (Cierco, 2018).

A verdade é que o pico dos números já está bem ultrapassado, no entanto, os anos de 2015 e 2016 demonstraram a fragilidade que as estruturas institucionais europeias tem, quando se trata da resolução de fluxos migratórios em massa. E a questão que se coloca é que estes fluxos, dependem diretamente da geografia securitária que se contempla nas regiões que circundam o Continente Velho. Vejamos o caso do despoletar da Guerra na Ucrânia, que fez aumentar drasticamente o fluxo de refugiados, vindos da Ucrânia.

Este enquadramento de análise, no que toca à geografia securitária, dos fluxos migratórios, permite analisar o fenómeno em causa como uma parte integrante do modelo europeu de segurança que Bruxelas procura implementar e, no limite, até exportar. Não só esse argumento é válido em termos de teóricos, como também no aspeto legal europeu. Ora, com a entrada em vigor do Tratado de Lisboa, e a subsequente eliminação da Europa dos Pilares de Maastricht, a Política de asilo e imigração passou a estar enquadrada também nas questões de segurança (Xavier, 2017).

Para esse efeito, quando a crise migratória de 2015 despoletou, a UE ganhou a capacidade de executar missões civis, militares e mistas, no âmbito da reação comunitária a este fenómeno. Assim, observou-se à securitização da migração.

Vejamos, então, quais desafios são causados pela migração em massa. Em primeiro lugar, tratou-se do Sistema Europeu de Asilo, que embora já tenha sido desenvolvido há vários anos, este ainda representava debilidades, quando se trata de receber um vasto número de refugiados (Cierco, 2018). Por outras palavras, a burocracia é lenta.

Não só as estruturas institucionais europeias mostraram vulnerabilidades, como também os agentes sociais e políticas tiveram reações muito adversas, que colocaram desafios fundamentais à própria ideia da União Europeia. Em primeiro lugar, o Eurobarómetro Standart de outubro de 2015 demonstrou que, para os europeus, a migração era o maior problema, até à data, que se colocava ao Estado da União, e subsequente, o sentimento de insegurança a que este estava ligado[1] (Xavier, 2017).

Em segundo lugar, a associação crescente entre os movimentos migratórios com a expansão do islamismo tem sido politicamente aproveitada por partidos políticos, sobretudo populistas, na sua essência, que se tornaram num forte pendor da extrema-direita, cuja ascensão veio acentuar o sentimento nacionalista e anti-imigração (Xavier, 2017).

Paralelamente, mas também consequentemente, receando que a incapacidade de gestão comunitária chegue a níveis muito elevados, vários países começaram a construir muros para controlar as fronteiras, com um objetivo inequívoco: impedir o fluxo de refugiados (Xavier, 2017).

Olhemos, então, para a estratégia que a UE lançou para colmatar estes desafios[2]. Logo em 2015, a 13 de maio, foi apresentada formalmente a Agenda Europeia para as Migrações, que estava baseada em 4 pilares:

- reduzir os incentivos à imigração ilegal;

- construir uma política de asilo sólida;

[1] Fazia-se aqui uma conexão direta entre o aumento dos ataques terroristas na Europa, com a chegada dos refugiados muçulmanos

[2] Não esquecendo que muitos desafios, como o da construção dos muros, por parte de alguns países, como foi caso da Hungria, também foi uma manifestação da falta de confiança na estratégia que a UE lançou.

- definir uma nova política em matéria de migração legal;

- salvar vidas humanas e garantir a segurança das fronteiras externas.

A implementação desta Agenda não foi imediata, mas sim faseada, tornou-se congruente com medidas de curto prazo, para estabilizar rapidamente a situação, e de longo prazo, com o fim de criar uma capacidade de resiliência dos mecanismos, para que possam resistir aos desafios operacionais.

Assim, observou-se um reforço de medidas em 5 patamares. Primeiro, a recolocação de refugiados, para aliviar a capacidade estrutural da Itália e da Grécia (países que estavam na linha da frente das receção dos mesmos). Em segundo lugar, a reinstalação de quase 20.000 pessoas oriundas de países terceiros que foram identificadas como prioritárias de proteção internacional. Seguidamente, a adoção de um plano de ação contra o tráfico de migrantes. Quarto, a criação de orientações para a recolha de impressões digitais dos migrantes, para garantir a sua entrada no Sistema Europeu Comum de Asilo. Por fim, em quinto lugar, uma consulta pública sobre o futuro da Diretiva do Cartão Azul (Xavier, 2017).

Assim, no que toca às medidas de curto prazo, em outubro é firmado um acordo de 17 pontos, entre o Presidente Juncker, da Comissão Europeia, com os Chefes de Estado dos países do Balcãs, para que fique estipulada a cooperação em matéria de gestão das fronteiras, de prestação de ajuda mútua e melhorar os canais de comunicação multilaterais. Neste panorama, ainda assim, a medida que mais impacto teve, foi o acordo firmado entre os Chefes de Estado e de Governo da UE e da Turquia, para que se garantisse a entrada de migrantes pelos canais juridicamente legais e o combate simultâneo com as redes de tráfico de migrantes (Xavier, 2017). De realçar, mais uma vez, que este acordo não foi assinado por nenhum oficial da UE, não sendo, desta forma, bilateral, mas sim, multilateral. Esta iniciativa, na qual a Alemanha teve um papel importante, deixou uma marca de tensão nas reuniões do Conselho Europeu.

No que toca à edificação de estruturas comunitárias de combate a este fenómeno – medidas de longo prazo, portanto. A Comissão Europeia adotou uma série de programas de cooperação transfronteiriça, para que fossem aplicados para o desenvolvimento económico e social das regiões de ambos os lados das fronteiras da União. Para além disso, é apresentada uma proposta de facilitar o intercâmbio de registos criminais,

dotando, assim, a Europol de instrumentos mais eficazes para a luta contra o crime transnacional organizado e o terrorismo (Xavier, 2017).

Por fim, a Comissão propõe a criação de uma Guarda Europeia Costeira e de Fronteiras, no seguimento da missão *Mare Nostrum* que a Marinha Italiana organizou, para poder impedir a travessia perigosa dos migrantes, pelo Mediterrâneo. Esta Guarda, que veio a assumir uma operação com o nome FRONTEX, tornou-se no instrumento comunitário, por excelência, que permitiu à UE a adoção de medidas de prevenção à morte de migrantes, durante a travessia (Xavier, 2017).

Com o objetivo de fortalecer e defender as fronteiras da UE, Jucker anuncia 5 medidas importantes. A edificação da Guarda Costeira, a definição de um sistema único de Entrada e Saída, a implementação de um Sistema Europeu de Informação e Autorização de Viagem, o reforço da Europol e o reforço de documentos de viagem seguros para uma melhor gestão da livre-circulação (Xavier, 2017).

De facto, perante a realidade apresentada, torna-se evidente que a União Europeia não precisa de reinventar a sua política de imigração e asilo, precisa de se esforçar no sentido de conseguir ter um consenso interno na matéria. Para isso, precisa de criar uma nova "diplomacia de fronteiras" (Xavier, 2017: 46), baseada em 3 níveis: nos países de origem, nos países de trânsito e nos países de destino. No primeiro caso, terá de ser feito através de uma intervenção no sentido de garantir condições de paz e segurança. No segundo, através da luta contra as redes de tráfico e crime organizado. Por último, através do incentivo à adoção de mais políticas de integração e não de assimilação (Xavier, 2017).

## 5. As respostas do Next Generation EU

O Next Generation EU, apesar de ser um programa temporário (2021- 2026) criado para lidar com as consequências da crise pandémica do Covid-19, pode-se tornar num marco histórico da criação de um novo modelo económico e fiscal vigente na União Europeia.

Para entender a forma como este modelo poderá quebrar com o modelo vigente, temos que fazer uma análise da sua adoção, à luz da liderança europeia face à crise da dívida pública de 2010, aquando da crise de 2008.

Vejamos, nos anos 2010, a UE adotou uma postura um pouco imoral face à resolução da crise do euro: cada governo nacional seria o responsável pelas suas próprias condições financeiras e políticas adotadas. Este paradigma é fundamentalmente adotado em federações, em que as relações entre as entidades heterogéneas são geridas pelo medo mútuo de que uns estados possam estar a compensar as perdas ou ganhos de outro estado, em termos económicos e demográficos (Buti e Fabrinni, 2023).

Porém, em termos da União Económica e Monetária (UEM), esse medo foi explorado pela lógica institucional. Para explicar melhor esta questão, é preciso voltar ao estabelecimento, em 1999, da UEM, que foi criada em duas lógicas paralelas, esta combinava uma lógica descentralizada, no que tocava a políticas fiscais e e económicas, que estavam sob a responsabilidade nacional, com uma lógica centralizante, no que constaria à política monetária, que era atribuída ao Banco Central Europeu. Pode-se mesmo dizer, que a UEM é o pináculo de um equilíbrio complexo entre duas formas de governação, que, por sua vez, causou estas preocupações morais com a adoção das medidas comunitárias face à Crise Soberana do Euro (Buti e Fabrinni, 2023).

Por sua vez, o Next Generation EU (NGEU) constituiu-se num aposta integrativa, por parte de Bruxelas, já que envolveu a Comissão Europeia a contrair massivos empréstimos nos mercados de capital, pela primeira vez na sua história (Buti e Fabrinni, 2023).

A observação do potencial que o NGEU pode oferecer à futura integração da União Europeia advém da análise de vários fatores. Assim, a conjugação de reformas nacionais, com a coordenação política e a integração institucional deverá procurar o aprofundamento dos poderes da Comissão e do Parlamento Europeu, que irá permitir ao NGEU passa o chamado "Teste de Compatibilidade de Monnet", que será visto como bem sucedido se se mantiver um equilíbrio entre a coerência política, económica e institucional (Buti e Fabrinni, 2023).

No que toca à aplicação de fundos do NGEU para o fortalecimento da questão da Migração e Gestão de Fronteiras, inseridas no âmbito "Make it Equal" do programa em questão, a União Europeia atribui a esta questão um total de 27.70 mil milhões de euros, divididos entre a Migração (cujo Fundo de Migração, Integração e Asilo receberá 9.88 mil milhões de euros e o Fundo Integrado de Gestão de Fronteiras receberá 6.25 mil milhões de euros) (Comissão, 2021).

Como foi firmado anteriormente, no que consta à gestão das migrações, também estamos perante uma questão de segurança, por isso deve-se somar o investimento da Comissão no Fundo Interno de Segurança, que rondará os 1.93 mil milhões, associado ainda a 7.95 mil milhões ao Fundo Europeu de Defesa e 1.69 mil milhões atribuídos à mobilidade militar (Comissão, 2021).

Não só se observa uma injeção na Migração e Segurança e Defesa, como também a orçamentação de 110.6 mil milhões a financiarem programas globais e da vizinhança, dos quais 95.75 mil milhões representarão um instrumento de financiamento de desenvolvimento regional na vizinhança e no mundo, enquanto 11.57 mil milhões irão para a Ajuda Humanitária e 2.68 mil milhões para a Política Comum de Segurança e Defesa (Comissão, 2021).

Temos, desta forma, duas perspetivas para analisar o sucesso do NGEU. Por um lado, o financiamento da chamada diplomacia de fronteiras, que vai permitir à UE uma intervenção a três níveis, sobre a resolução das vulnerabilidades colocadas pelas migrações. Em segundo lugar, a sua materialização institucional e a nível comunitário que poderão representar uma mudança de paradigma na governança europeia, em matéria económica. Poderemos ver o sucesso do NGEU se a Comissão for capaz de usar os recursos oferecidos para potenciar a convergência política dos Estados-Membros sobre as políticas comunitárias.

## Bibliografia

Buti, Marco & Fabbrini, Sergio, (2023) *Next generation EU and the future of economic governance: towards a paradigm change or just a big one-off?*, Journal of European Public Policy, Vol. 30: 4, 676-695.

Cierco, Teresa, (2018) *Fluxos Migratórios e sua Gestão: Perspetiva Europeia*, Coleção de Policy Papers, Fundação Konrad Adenauer, Botafogo, Brasil.

Comissão Europeia, (2021) *The EU's 2021-2027 long-term Budget and NextGenerationEU: Facts and Figures*, Publication Office of the European Union, Luxemburgo.

Disponível em: https://www.ohchr.org/en/statements/2022/09/human-rights-concerns-related-forced-displacement-ukraine

ICRC, (2015) Direito Internacional Humanitário (DIH): Resposta às suas perguntas, Genebra

ICRC, (2019) Displacement in Times of Armed Conflict: How International Humanitarian Law protects in war, and why it matters, Genebra.

Kehris, 2022, Human Rights concerns related to forced displacement in Ukraine, OHCHR, Reunião do Conselho de Segurança sobre a Ucrânia

Parrish, Filo, (2022) Conflict in Ukraine: What do we know about the internal displacement situation so far?

V. Rabus, 2022 Addressing Internal Displacement in Ukraine, Georgetown University

Xavier, Ana Isabel, (2017) *A União Europeia, migrações e (in)segurança: estratégias, vulnerabilidades e desafios*, Perspectivas, Journal of Political Science, Vol. 16.

# O papel da tecnologia e do digital na promoção da economia sustentável: desafios e oportunidades para a UE

Clara Ribeiro, Fac. Direito Univ. NOVA de Lisboa

Guilherme Taxa, Universidade Católica Portuguesa

## Resumo

Estando na vanguarda da adoção de políticas "climate friendly", bem como no estabelecimento de metas ambiciosas, com o objetivo de uma posição de assumir e reforçar liderança e de exemplo no contexto mundial. Ainda assim, entre os vários desafios que atormentam esta transição, o setor económico, nas suas mais variadas dimensões, sofre com os impactos que estas políticas possam causar. Neste sentido, a tecnologia e o digital desempenham um papel fundamental para minimizar os impactos desta alteração de políticas e comportamentos, contribuindo para a redução dos gases com efeito de estufa e outros, concretizando adaptações necessárias e alargando o leque de opções viáveis, numa perspetiva em que facilita a mitigação dos efeitos indesejáveis das soluções na economia em geral e, sobretudo, nos setores de risco e de forma a concretizar a meta de uma economia sustentável. Embora a digitalização da economia apresente oportunidades para o desenvolvimento sustentável e para uma robustez económica, verificam-se alguns desafios que, persistentemente, atrasam o processo e cuja resolução nem se sempre se adivinha fácil.

**Palavras-Chave:** Economia Digital, Economia Sustentável, Ambiente, Transformação Digital, NextGenerationEU

# 1. Introdução

O ambiente surge como tema prioritário na agenda da União Europeia (EU), nomeadamente no que diz respeito às alterações climáticas, às emissões de gases poluentes e, consequentemente, às alternativas existentes com vista a fazer face a este problema. A UE encontra-se, portanto, na vanguarda da adoção de políticas "climate friendly", bem como no estabelecimento de metas ambiciosas acordadas entre estados soberanos, assumindo uma posição de liderança e de exemplo no contexto mundial. Ainda que a evidência de estarmos perante um problema seja clara, é relevante ter em conta que, entre os vários desafios que atormentam esta transição, o setor económico, nas suas mais variadas dimensões, sofre diretamente com o impacto das sucessivas políticas. De facto, uma economia empresarial assente numa política de baixos níveis de carbono, por exemplo, enfrenta desafios a algumas indústrias mais poluentes fortemente dependentes de práticas e recursos ditos convencionais. Neste sentido, a tecnologia e o digital desempenham um papel fundamental para minimizar os impactos desta alteração de políticas e comportamentos, contribuindo para a redução dos gases com efeito de estufa e outros, concretizando adaptações necessárias e alargando o leque de opções viáveis, numa perspetiva em que facilita a mitigação dos efeitos indesejáveis das soluções na economia em geral e, sobretudo, nos setores de risco e de forma a concretizar a meta de uma economia sustentável.

# 2. Economia Digital Sustentável

## a) Relação entre a Economia Digital e a Economia Ecológica no contexto da UE

Os principais objetivos da UE a longo prazo consistem, sobretudo, na redução das emissões de gases de efeito de estufa (doravante 'GEE'), de modo a atingir a neutralidade climática, bem como na digitalização da economia. Estes dois processos não devem ser considerados de forma independente, uma vez que a digitalização da economia não é mais do que um meio para atingir a neutralidade climática (Kuzior et al., 2022). A economia ecológica visa restaurar o crescimento económico e, simultaneamente, agir face às alterações climáticas e a outros fenómenos da sustentabilidade ambiental. Como tal, a economia digital promove a economia ecológica, uma vez que está presente em todos os domínios importantes da sociedade e visa promover a reconstrução da agenda política de

modo a integrar o impacto ambiental das tecnologias digitais. Surge, assim, o conceito de "economia digital sustentável" enquanto solução para os problemas ambientais que integra a criatividade e o dinamismo da economia digital para benefício, não só do setor económico, mas também do ambiente e da sociedade. (Ciocoiu, 2011)

Efetivamente, o comprometimento da UE com a transformação digital e ecológica dos Estados e das empresas que a compõem é visível não só nos documentos emitidos pela Comissão Europeia, mas também na Declaração sobre Uma Transformação Ecológica e Digital para a UE. Esta declaração foi assinada em 2021 por 24 Estados Membros da UE, bem como pela Noruega e a Islândia, na qual os mesmos se comprometeram a acelerar a implementação de tecnologias verdes. Do mesmo modo, o European Green Deal, aprovado em 2020, implementou uma nova estratégia de crescimento para uma transformação dupla - ecológica e digital - que visa transformar a UE numa sociedade justa e próspera, com uma economia competitiva, climaticamente neutra e eficiente (Bednarčíková & Repiská, 2021). Contudo, é importante ressalvar que este nexo ambiente-tecnologia esteve sempre presente no Direito da União Europeia. O Tratado sobre o Funcionamento da União Europeia (doravante 'TFUE') estabelece que, aquando da elaboração da política de domínio ambiental, a UE deverá ter em conta os dados científicos e técnicos de que dispõe.[1] Além disso, também a Carta dos Direitos Fundamentais da União Europeia estabelece a necessidade de proteger os direitos fundamentais de acordo com o progresso social, científico e tecnológico.[2] (Aragão, 2019)

É neste contexto que surge o conceito de transformação digital ecológica, processo de mudança profunda que visa implementar a digitalização dos processos de negócio, atividades, produtos e modelos de modo a tornar as empresas mais sustentáveis a nível ambiental. A promoção da eficiência, inovação, competitividade e do crescimento económico da empresa é aqui articulada com a diminuição da poluição, a eficiência energética e a eficácia na alocação de recursos (Bednarčíková & Repiská, 2021).

### b) Oportunidades e Desafios

É amplamente aceite que as novas tecnologias têm impactos positivos e negativos nas relações económicas e sociais e, sobretudo, no ambiente. Como tal, a análise do impacto ambiental do desenvolvimento tecnológico deverá ter em consideração vários aspetos.

Em cada estado de evolução, o desenvolvimento tem impactos tanto negativos como positivos nos três pilares do desenvolvimento sustentável: a economia, a sociedade e o ambiente. Além disso, a digitalização está presente em todos os setores da economia e em todos os domínios da sociedade, influenciando a vida quotidiana, os modelos de negócio e o modo de pensar e agir na política. Devido ao papel central das TIC na economia, o impacto da crise económica nas mesmas é duplo, isto é, tem impactos diretos e indiretos não só no próprio setor das TIC, mas também na utilização produtiva e inovadora dessas tecnologias em toda a economia e sociedade. (Ciocoiu, 2011)

As tecnologias digitais limpas, quando implementadas de forma inteligente, promovem a eficiência energética, facilitam a economia circular, reduzem a poluição, a perda de biodiversidade e a degradação ambiental e aumentam a resiliência face ao impacto das alterações climáticas. Desta forma, contribuem para a ação climática e a sustentabilidade ambiental, conduzindo ao alcance dos Objetivos de Desenvolvimento Sustentável da ONU (Ministerial Declaration). A digitalização tem um elevado potencial a longo prazo nas empresas e a sua ampla compatibilidade permite que a mesma possa ser aplicada em quase todas as indústrias e a vários processos de negócio (Bednarčíková & Repiská, 2021).

Neste contexto, é importante realçar o papel da Inteligência Artificial (doravante 'IA'), cuja aplicação ambiental em quatro setores – agricultura, energia, água e transportes – poderá conduzir ao aumento do PIB mundial em 4.4% até 2030, 5.5% na Europa, bem como a uma redução nas emissões de GEE em 4% até 2030 (Bednarčíková & Repiská, 2021).

Apesar de todos os benefícios que o processo de digitalização da economia apresenta, existem ainda muitas desvantagens associadas ao mesmo. O grau de desenvolvimento necessário ao desencadeamento de uma produção sustentável, o impacto ecológico pelo qual este processo ainda é responsável, os custos associados à implementação do mesmo e as desigualdades económicas e sociais que afetam a sua implementação são alguns dos inconvenientes identificados.

A economia digital, nomeadamente as Tecnologias de Informação e Comunicação (doravante 'TIC'), são responsáveis pela criação de oportunidades para o desenvolvimento sustentável e a recuperação económica nas recentes crises. Contudo, o

progresso tecnológico que a mesma representa leva o setor empresarial a redefinir e aumentar a produção o que, inicialmente, se reflete no aumento das emissões de CO2 (Li et al., 2021). Apenas quando a digitalização atinge um nível suficientemente elevado, é que a quantidade de CO2 manuseada supera aquela que é emitida, uma vez que as empresas produzem os bens a um nível estável, permitindo que o progresso tecnológico se reflita numa economia ecológica (Kuzior et al., 2022).

O impacto ecológico destas tecnologias não fica por aqui. Atualmente, as tecnologias digitais consomem entre 8 e 10% da eletricidade e são responsáveis por 2 a 4% das emissões globais de GEE. Estas pequenas percentagens, acabam por se refletir em grandes números (Comissão Europeia, 2023) e, na ausência de vigilância, a pegada ecológica do setor poderá aumentar para 14 % das emissões globais até 2040 (Comissão Europeia, 2020). Além disso, várias empresas usam tecnologias desatualizadas, que carecem de eficiência e informação acerca do seu impacto no ambiente. Desta forma, as empresas acabam a prejudicar o ambiente sem, muitas vezes, sequer se aperceberem disso (Bednarčíková & Repiská, 2021).

Os custos iniciais necessários à criação de empresas economicamente ecológicas são bastante elevados, especialmente os relacionados com a produção de energia. A investigação e o desenvolvimento no domínio das energias renováveis são muito dispendiosos e encontram-se, ainda, numa fase bastante embrionária (Ciocoiu, 2011). É por este motivo que se verifica uma elevada disparidade dos efeitos provocados pela digitalização da economia nas regiões mais desenvolvidas quando comparadas com as menos desenvolvidas. Na China, observou-se que a economia digital tem um efeito positivo no ambiente nas regiões desenvolvidas do país e um efeito negativo nas regiões menos desenvolvidas (Li et al., 2021). As regiões economicamente subdesenvolvidas apresentam um desenvolvimento tardio do processo de digitalização, enquanto nas regiões economicamente mais desenvolvidas as empresas têm elevada capacidade de inovação e aplicação da tecnologia digital. Desta forma, a economia digital acaba por favorecer apenas as regiões mais desenvolvidas, cujas empresas possuem uma maior probabilidade de ocupar uma posição dominante no mercado (He et al., 2023).

# 3. Implementação de Medidas Ambientalmente Sustentáveis na Economia - Análise Setorial

## a) Energias renováveis

O uso de energias renováveis oferece uma alternativa sustentável aos combustíveis fósseis, desempenhando um papel significativo na redução das emissões de gases com efeito de estufa na UE. Nos últimos anos foi registado um aumento significativo do recurso a fontes de energia renováveis, incluindo a eólica, a solar e a biomassa. A energia eólica registou um crescimento substancial, com o desenvolvimento de parques eólicos offshore e a expansão de instalações "onshore" (IRENA, 2022). Além disso, a energia solar fotovoltaica ganhou proeminência, com a instalação de painéis solares em residências particulares e em projetos à escala de serviços públicos; a energia da biomassa, que deriva de materiais orgânicos, contribuiu, da mesma forma, para a descarbonização do sector energético, fornecendo outra alternativa (EurObserv'ER, 2021).

Neste aspeto, o desenvolvimento tecnológico foi e permanece essencial para o desenvolvimento das energias renováveis em termos da sua eficácia e eficiência: "While incremental innovation is important for the improvement of specific renewable energy technologies (e.g. by scaling up the size of offshore wind turbines), more radical innovations such as the development of smarter, more flexible electricity systems can help to integrate variable renewable technologies in greater proportions or at a lower cost than was previously thought possible" (Dong Wu, et al., 2019). O impacto da utilização de energias renováveis no tecido empresarial pode ser considerável se permitir a redução de custos, uma maior independência energética ou o acesso a incentivos e subsídios estatais, permitindo dar continuidade à atividade em causa sem um custo ambiental associado.

## b) Captura, utilização e armazenamento de carbono (CCUS)

As tecnologias de captura, utilização e armazenamento de carbono (CCUS) oferecem uma solução interessante para as emissões poluentes geradas pelas indústrias e centrais elétricas na UE. Os sistemas CCUS envolvem a captura das emissões de dióxido de carbono (CO2), o seu transporte e o seu armazenamento subterrâneo seguro ou a sua

utilização para outros fins. Estas tecnologias evitam que o CO2 seja libertado para a atmosfera, reduzindo assim as emissões de gases com efeito de estufa. A UE encontra-se a investir ativamente no desenvolvimento e implantação de tecnologias CCUS para apoiar a transição para uma economia de baixo carbono (Comissão Europeia, 2020), sendo que desta forma permite adotar uma medida, provisória ou não, que limita os níveis de emissões sem colocar em causa a sustentabilidade de alguns setores e empresas como as centrais a carvão que, em alguns locais, continuam a ser fulcrais para o fornecimento completo às populações.

### c) Soluções de transporte sustentáveis

Os transportes assumem-se ainda como um dos principais responsáveis pelas emissões de gases com efeito de estufa na União Europeia. As inovações tecnológicas no sector dos transportes são vitais para alcançar uma mobilidade sustentável e reduzir as emissões. Os veículos elétricos, no presente momento, ganham força como uma alternativa eficaz aos veículos convencionais com motor de combustão. Neste sentido, a UE tem vindo a promover a adoção deste tipo de veículos através de incentivos, nomeadamente através de benefícios fiscais e do desenvolvimento de infraestruturas, com o objetivo de facilitar a transição para um sistema de transportes mais limpo (Comissão Europeia, 2021).

Adicionalmente, os avanços na tecnologia das baterias e a criação de infraestruturas de carregamento são essenciais para o triunfo dos veículos elétricos no mercado automóvel, tendo em conta que, para além destes, existem ainda outros obstáculos ao sucesso desta alternativa, nomeadamente no que concerne ao transporte de mercadorias. Se eventualmente o transporte rodoviário poderá já ter encontrado uma solução para o presente cenário (não sendo tão certo assim que a eletrificação dos veículos atinja eficazmente o transporte rodoviário de mercadorias), a realidade demonstra que os transportes aéreos, ferroviários e marítimos, indispensáveis nesta área, enfrentam ainda dificuldades relativamente à redução da sua mancha ambiental. Assim, não é evidente que surja, a curto prazo, uma resposta séria aos olhos das empresas que seja capaz de fazer oposição a esta problemática, apesar dos consideráveis avanços na área do hidrogénio.

### d) Eficiência energética e redes inteligentes

A melhoria da eficiência energética é também um passo fundamental no seio da questão e deve ser alcançada por todos os setores da sociedade. Os avanços tecnológicos em edifícios e indústrias eficientes do ponto de vista energético podem contribuir significativamente para este objetivo. Os sistemas de edifícios inteligentes, incluindo sistemas de AVAC (aquecimento, ventilação e ar condicionado), sensores de ocupação e sistemas de gestão da energia, potencializam o consumo de energia e reduzem os resíduos (IEA, 2020). Além disso, os processos industriais podem ser aprimorados através da integração de tecnologias energeticamente eficientes, tais como sistemas de controlo avançados, recuperação de calor residual e cadeias de abastecimento otimizadas, bem como através da integração de redes inteligentes, que permitem uma melhor gestão e distribuição de energia, facilitando a integração de fontes de energia renováveis e promovendo a eficiência energética. Verifica-se portanto que as empresas devem olhar para a transição energética como uma oportunidade de expansão, deixando para outro plano os entraves iniciais que a preocupação climática terá provocado em alguns casos.

### e) Transformação económica impulsionada pela tecnologia

Embora as políticas respeitadoras do clima possam inicialmente perturbar determinados sectores, a tecnologia oferece oportunidades de transformação económica e de crescimento na UE. A adoção e o desenvolvimento de tecnologias inovadoras geram novas oportunidades de negócio e promovem a criação de emprego. Os investimentos em tecnologias limpas e em infraestruturas de energias renováveis criam perspetivas de emprego, atraem investimentos e estimulam o desenvolvimento económico. Da mesma forma, a tecnologia permite que as empresas se adaptem a políticas favoráveis ao clima, implementando práticas eficientes do ponto de vista energético ao adotar métodos de produção sustentáveis, ao explorar novos mercados e sabendo que ao abraçar os avanços tecnológicos, poderão aumentar a sua competitividade, reduzir custos e alinhar-se com os objetivos de sustentabilidade.

## 4. Conclusão

Em conclusão, podemos afirmar que o conceito de uma economia digital sustentável surge como uma das soluções para os desafios ambientais, integrando a criatividade e o

dinamismo das tecnologias digitais em benefício da economia, do ambiente e da sociedade. No entanto, embora a digitalização da economia apresente oportunidades para o desenvolvimento sustentável e para uma robustez económica, verificam-se alguns desafios que, persistentemente, atrasam o processo e cuja resolução nem se sempre se adivinha fácil. A abordagem atenta dos impactos ambientais, a promoção de tecnologias limpas e a atenuação das desigualdades que condicionam a democratização do esforço pelo ambiente são essenciais para alcançar uma transformação digital e tecnológica sustentável e equitativa. O equilíbrio entre os benefícios e os desafios da digitalização e as preocupações ambientais será crucial para moldar um futuro em que o crescimento económico e a sustentabilidade ambiental caminhem lado a lado.

A tecnologia desempenha portanto um papel central na atenuação dos impactos das políticas favoráveis ao clima nos sectores poluentes, em especial no que respeita à redução de emissões, na União Europeia. A tecnologia de energias renováveis, as CCUS, as soluções de transporte sustentáveis e as práticas energeticamente eficientes são cruciais para atingir os objetivos ambientais propostos e, ao mesmo tempo, promover o crescimento económico. Ao tirar partido da tecnologia, a UE pode enfrentar com êxito os desafios colocados por políticas climáticas que ameaçam alguns setores económicos e que representam dificuldades acrescidas para outros, redirecionando a estratégia a ser seguida pelo tecido empresarial e transacionado para uma economia com baixas emissões de carbono de forma a garantir um futuro sustentável.

## Bibliografia

A Green and Digital Transformation of the EU Ministerial Declaration. Digital Day 2021 March 19th. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDQxMwMAT7AwdwUAAAA%3D

Aragão, A. (2019). Digital tools for a greener Europe: democracy, environmental justice, and sustainability in the EU through information and communication technologies and geographic information systems. UNIO - EU Law Journal, 5, 85-91. https://revistas.uminho.pt/index.php/unio/article/view/253

Bednarčíková D., Repiská R. (2021). Digital Transformation in the Context of the European Union and the Use of Digital Technologies as a Tool for Business Sustainability. Current Problems of the Corporate Sector. https://doi.org/10.1051/shsconf/202111501001

Betting on the future of automobiles. (2023). KPMG. https://kpmg.com/xx/en/home/insights/2021/07/betting-on-the-future-of-automobiles.html

Carbon capture, Storage and Utilisation. (2020). European Commission. https://energy.ec.europa.eu/topics/oil-gas-and-coal/carbon-capture-storage-and-utilisation_en\

CIOCOIU, C. (2011). Integrating Digital Economy and Green Economy: Opportunities for Sustainable Development. Theoretical and Empirical Researches in Urban Management, 6(1), 33-43 https://www.jstor.org/stable/10.2307/24873273

Energy Efficiency. (2020). IEA. https://www.iea.org/topics/energyefficiency

Green digital sector. (2023). European Commission. https://digital-strategy.ec.europa.eu/en/policies/green-digital

He Y., Zhang Y. , Huang W., Wang R., He L., Li, B., Zhang Y. (2023). Impact of digital economic development and environmental pollution on residents' health: an empirical analysis based on 279 prefecture-level cities in China. BMC Public Health. https://doi.org/10.1186/s12889-023-15788-4

Kovacikova M., Janoskovaa P., Kovacikova K. (2021). The Impact of Emissions on the Environment within the Digital Economy. Transportation Research Procedia, 55, 1090-1097. https://doi.org/10.3390/su13137267

Kuzior A., Vyshnevskyi O., Trushkina N. (2022). Assessment of the Impact of Digitalization on Greenhouse Gas Emissions on the Example of EU Member States. Production Engineering Archives, 28(4), 407-419. https://doi.org/10.30657/pea.2022.28.50

Li X., Liu J., Ni P. (2021). The Impact of the Digital Economy on CO2 Emissions: A Theoretical and Empirical Analysis. Sustainability, 13, 7267. https://doi.org/10.3390/su13137267

Mobility and Transport. (2021). European Commission. https://ec.europa.eu/transport/themes/mobilitystrategy_en

Renewable Energies: The Future of Energy Supply. (2021). Energynautics Biomass Energy. https://energynautics.com/en/branches/renewable-energies/ /

Shaping Europe's digital future. (2020). European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en

Smart Grids. (2019). Energynautics https://www.energynautics.com/smart-grids/

Supporting The Green Transition. (2020). European Commission. https://ec.europa.eu/commission/presscorner/detail/en/fs_20_281

Wind Energy. (2022). IRENA. https://www.irena.org/wind

Wu, D., Bokor, K., Helser, J. H., Miedzinski, M., & Ting, B. T. (2019). The Role of Science, Technology and Innovation in Promoting Renewable Eenergy by 2030. UNCTAD. https://unctad.org/system/files/officialdocument/dtlstict2019d2_en.pdf

# BOLETIM TERTÚLIA

## Encontros e Reflexões

SEGURANÇA E DEFESA EUROPEIA

VOLUME 1

**PLANO DE RECUPERAÇÃO E RESILIÊNCIA**

OBJETIVOS E DESAFIOS ESTRATÉGICOS

Segue-nos em::

@eurodefensejovem

@eurodefensejovem-portugal5469

linktr.ee/eurodefenseportugal

eurodefenseportugal

Contacta com a EuroDefense-Jovem através de:

jovem@eurodefense.pt

COM O APOIO

REPÚBLICA PORTUGUESA
DEFESA NACIONAL