



Revista Científica del Centro Universitario de la Guardia Civil

Revista **Lógos** Guardia Civil

Versão
Português

Vol. 3 Núm. 2 (2025)
junho

RESUMO

I.- COLABORAÇÕES

LCooperação em matéria de aplicação da lei e ação penal: construção paralela?

Adriano J. Alfonso Rodríguez

II.- TRABALHO DE INVESTIGAÇÃO

A Espanha face à desinformação: desafios híbridos e respostas convencionais

Juan Francisco Adame Hernández

A inteligência em foco: da teoria clássica a uma nova abordagem de implementação na era digital

Paula Castro Castañer

Hacktivismo: do protesto social à instrumentalização do Estado

IProteção internacional e soberania: o difícil equilíbrio entre direitos individuais e segurança nacional

Alejandro Gómez García

NA guerra de Nixon contra a droga e o aumento da vigilância virtual das fronteiras nos Estados Unidos

J. Luigi M. Kunz Saponaro

Violência sexual por parte de estranhos em Madrid e Barcelona: uma análise situacional

Francisco Pérez-Fernández/ Heriberto Janosch/ Enrique López López/ Francisco López-Muñoz

Drogas e condução: "Tolerância zero". Metodologia do relatório salivar do laboratório Synlab e critérios de aprovação da Entidade Nacional de Acreditação

Juan Carlos Rodríguez Bello

Proteção das infra-estruturas submarinas críticas e reforço da segurança do Mar Báltico: a operação

Baltic Sentry da NATO

Mónica Román González

IO capital intelectual na Instituição da Guardia Civil e o seu contributo para a economia social

Virginia Belén Subirís Moriel

III.- ANÁLISE DA JURISPRUDÊNCIA

Revista de Jurisprudência 2ª Secção Supremo Tribunal de Justiça





Edita:

Ministério do Interior. Secretariado Técnico Geral. Madrid.

Catálogo de Publicações da Administração Geral do Estado: <https://cpage.mpr.gob.es>.

Logótipos Revista Guardia Civil

Revista científica do Centro Universitário da Guarda Civil

Data de edição: junho de 2025

NIPO (papel): 126-23-018-2

NIPO (em linha): 126-23-019-8

Depósito legal: M-3619-2023

ISSN: 2952-3249

ISSN em linha: 2952-394X

Entidade responsável:

Centro Universitário da Guardia Civil

Área de investigação

Paseo de la Princesa, s/n

28300 Aranjuez (Madrid)

correio eletrónico: investigacion@cugc.es

Conceção e apresentação:

Gabinete da Área de Investigação

As opiniões expressas nesta publicação são da exclusiva responsabilidade dos autores.

A publicação desta revista e a sua divulgação é efectuada de acordo com as políticas de acesso aberto à produção científica. Desta forma, e com o objetivo de disponibilizar o conhecimento a toda a sociedade, esta revista publica gratuitamente todos os artigos e outros conteúdos digitais ao abrigo de uma licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) (<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

DIRECTOR

Dr. Félix Blázquez González. Tenente-General da Guarda Civil. Diretor do CUGC.

CHEFE DE REDACÇÃO

Blas Guillamón Campos. Tenente-coronel da Guarda Civil. CUGC.

SECRETÁRIO

Oliver Cadenas Roldán. Comandante da Guardia Civil CUGC.

COMITÉ EDITORIAL

Dr. Félix Blázquez González. Tenente-General da Guarda Civil. Dtor. CUGC.

Blas Guillamón Campos. Tenente-coronel da Guarda Civil. CUGC.

Dr. Carlos Fernández Liesa. Professor de Direito Internacional Público e Relações Internacionais. Delegado da UC3M no CUGC.

Dra. Ana M^a Garrocho Salcedo. Vice-Decana de Estudos Internacionais - Direito UC3M.

Dr. Francisco López Muñoz. Professor de Farmacologia. Vice-Reitor de Investigação e Ciência - UCJC.

Dra. Clara Sainz de Baranda Andujar. Diretora do Instituto de Estudos de Género - UC3M.

Dr. Manuel Díaz Martínez. Professor de Direito Processual - UNED.

Dr. Jordi Gimeno Beviá. Vice-Diretor de Investigação e Internacionalização. Faculdade de Direito - UNED.

Dr. Ricardo Cuevas Campos. Vice-reitor de Política Científica - UCLM

Dra. Amaya Arnáiz Serrano. Subdiretora do Instituto Alonso Martinez de Justiça e Contencioso - UC3M.

Dr. Cástor M. Díaz Barrado. Professor de Direito Internacional Público e Relações Internacionais - URJC.

Carlos Berbell Bueno. Jornalista. Diretor do Jornal Confilegal.

Oliver Cadenas Roldán. Comandante da Guardia Civil. Secretário.

COMITÉ CIENTÍFICO

Dr. Félix Blázquez González. Tenente-General da Guarda Civil. Diretor do CUGC.

Dr. Anselmo del Moral Torres. Coronel da Guardia Civil. Diretor Executivo do CUGC.

Dr. Eduardo Martínez Viqueira. Chefe Geral do Comando Pessoal da Guardia Civil.

Jacobo Barja de Quiroga López. Juiz Presidente da 5^a Secção do Supremo Tribunal de Justiça.

Julián Sánchez Melgar. Juiz. Segunda Secção do Supremo Tribunal de Justiça.

Dr. Juan Díez Nicolás. Professor de Sociologia. Membro da Real Academia de Ciências Morais e Políticas.

Dr. Juan Aparicio Barrera. Editor da revista Logos Science & Technology. Colômbia.

Dr. Pablo Morenilla Allard. Professor de Direito Processual - UCLM.

Dr. Jacobo Dopico Gómez-Aller. Professor de Direito Penal - UC3M.

Dr. Fernando Bandrés Moya. Professor de Medicina Legal - UCM.

Blas Guillamón Campos. Tenente-coronel da Guarda Civil. CUGC.

Oliver Cadenas Roldán. Comandante da Guardia Civil. Secretário.

Sítio Web oficial Logos Revista Guardia Civil

<https://revistacugc.es>



Sítio Web oficial do CUGC

<https://www.cugc.es>





ÍNDICE

INTRODUÇÃO	9
------------------	---

I.- COLABORAÇÕES

Cooperação em matéria de aplicação da lei e ação penal: construção paralela?.....	13
<i>Adriano J. Alfonso Rodríguez</i>	

II.- TRABALHO DE INVESTIGAÇÃO

A Espanha face à desinformação: desafios híbridos e respostas convencionais	37
<i>Juan Francisco Adame Hernández</i>	
A inteligência em foco: da teoria clássica a uma nova abordagem de implementação na era digital.....	71
<i>Paula Castro Castañer</i>	
Hacktivismo: do protesto social à instrumentalização do Estado	101
<i>Josué Expósito Guisado</i>	
Proteção internacional e soberania: o difícil equilíbrio entre direitos individuais e segurança nacional	123
<i>Alejandro Gómez García</i>	
A guerra de Nixon contra a droga e o aumento da vigilância virtual das fronteiras nos Estados Unidos	147
<i>J. Luigi M. Kunz Saponaro</i>	
Violência sexual por parte de estranhos em Madrid e Barcelona: uma análise situacional.....	171
<i>Francisco Pérez-Fernández / Heriberto Janosch / Enrique López López / Francisco López-Muñoz</i>	
Drogas e condução: "Tolerância zero". Metodologia do relatório salivar do laboratório Synlab e critérios de aprovação da Entidade Nacional de Acreditação.	197
<i>Juan Carlos Rodríguez Bello</i>	

Proteção das infra-estruturas submarinas críticas e reforço da segurança do Mar Báltico: a operação Baltic Sentry da NATO	221
<i>Mónica Román González</i>	

O capital intelectual na Instituição da Guarda Civil e o seu contributo para a economia social	257
<i>Virgínia Belén Subiris Moriel</i>	

III.- ANÁLISE DA JURISPRUDÊNCIA

Revista de Jurisprudência 2ª Secção Supremo Tribunal de Justiça	295
<i>Javier Ignacio Reyes López</i>	



INTRODUÇÃO

Caro leitor,

É com grande satisfação que lhe damos as boas-vindas à quinta edição da nossa revista Logos Guardia Civil, editada pelo Centro Universitário da Guardia Civil. Esta nova edição reúne uma seleção de trabalhos que abordam, a partir de diferentes abordagens e disciplinas, alguns dos desafios mais prementes no âmbito da segurança, tanto nacional como internacional.



Abrimos esta edição com a colaboração de Adriano J. Alfonso Rodríguez, Doutor em Direito e Professor de Direito-Criminologia da UNED, que nos oferece uma reflexão oportuna sobre a «Cooperação entre agências de segurança e processos de integração regional na América Latina».

Na secção de artigos de investigação, Juan Francisco Adame Hernández, Diretor de Estratégia, Comunicação e Promoção da Casa Árabe, apresenta-nos «Espanha face à desinformação: desafios híbridos e respostas convencionais», um estudo rigoroso sobre os riscos da desinformação para a segurança do Estado.

A especialista em segurança e doutoranda em Ciências Forenses pela Universidade de Alcalá, Paula Castro Castañer, introduz-nos em «A inteligência no ponto de mira: da Teoria Clássica à implementação na Era Digital», uma abordagem crítica sobre a perceção social dos serviços de inteligência.

O trabalho de Josué Expósito Guisado, sargento da Guardia Civil e doutorando na Universidade Pablo de Olavide, intitulado «Hacktivismo: da protesto social à instrumentalização estatal», analisa os limites entre a ação digital e a ilegalidade penal.

Alejandro Gómez García, capitão da Guardia Civil e mestre em Gestão Operativa da Segurança, aprofunda a «Proteção internacional e soberania: o complicado equilíbrio entre direitos individuais e segurança nacional», uma questão de grande sensibilidade no direito internacional.

Don Johannes Luigi Maria Kunz Saporano, investigador doutoral na Universidade Carlos III de Madrid, analisa no seu artigo «A guerra de Nixon contra as drogas e o auge da vigilância virtual nas fronteiras dos Estados Unidos» a transformação da segurança nos EUA, apontando como as políticas impulsionadas durante a «guerra contra as drogas» deram lugar ao desenvolvimento de sofisticados sistemas de controlo fronteiriço apoiados em tecnologia avançada.

A equipa formada por Francisco Pérez-Fernández, Heriberto Janosch, Enrique López López e Francisco López-Muñoz apresenta «Violência sexual exercida por desconhecidos em Madrid e Barcelona: uma análise situacional», um estudo que fornece informações relevantes sobre a distribuição geográfica e os padrões de comportamento em agressões sexuais urbanas.

Juan Carlos Rodríguez Bello, Cabo 1º da Agrupación de Tráfico da Guardia Civil, especialista universitário em Delinquência Rodoviária e Perito Judicial em Documentoscopia pela UNED, assina o artigo «Drogas e condução: Tolerância zero. Metodologia do relatório salivar do laboratório Synlab e critérios de homologação da Entidade Nacional de Acreditação», onde são abordados os padrões científicos e legais na deteção de substâncias.

Mónica Román González é doutoranda no Programa de Ciências Políticas e da Administração e Relações Internacionais da Universidade Complutense de Madrid e oferece-nos uma análise estratégica em «A proteção das infraestruturas submarinas críticas e o reforço da segurança do mar Báltico: a operação Baltic Sentry da OTAN», destacando a importância da cooperação internacional em cenários marítimos.

Para terminar, Virginia Belén Subiris Moriel, doutoranda na Universidade Rey Juan Carlos, Programa de Ciências Sociais e Jurídicas, encerra com «Economia Social: A contribuição da Instituição da Guarda Civil através do seu capital intelectual», um artigo que explora o valor do conhecimento partilhado e o compromisso institucional com o desenvolvimento social.

Por outro lado, a secção de resenhas jurisprudenciais conta, nesta ocasião, com uma nova contribuição de Javier Ignacio Reyes López, Magistrado Juiz Decano de Alcalá de Henares, que analisa sentenças relevantes da Segunda Secção do Supremo Tribunal.

O comité editorial agradece sinceramente aos autores pelo seu rigor e empenho, bem como aos avaliadores externos pelo seu trabalho indispensável. Esperamos que esta nova edição seja do vosso interesse e contribua para o conhecimento, a reflexão e a melhoria contínua no campo da segurança.

Félix Blázquez González
Diretor do CUGC



I.- COLABORAÇÕES



Colaboração

COOPERAÇÃO EM MATÉRIA DE APLICAÇÃO DA LEI E ACÇÃO PENAL: CONSTRUÇÃO PARALELA?

Tradução para o português com ajuda de IA (DeepL)

Adriano J. Alfonso Rodríguez
Doutor em Direito
Professor de Direito-Criminologia UNED-Lugo. Juiz(es)
ajalfonsorodriguez@hotmail.com
ORCID: 0009-0005-2821-4603

Recebido a 14/05/2025
Aceite em 14/05/2025
Publicado em 27/06/2025

Citação recomendada: Afonso, A. J. (2025). Cooperação entre as forças da ordem e a ação penal: Construção Paralela? *Revista Logos Guardia Civil*, 3(2), p.p. 13-34.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

COOPERAÇÃO EM MATÉRIA DE APLICAÇÃO DA LEI E ACÇÃO PENAL: CONSTRUÇÃO PARALELA?

Resumo: PREFÁCIO. 2. O MODELO DE AUTORIZAÇÃO JUDICIAL PARA AS ACTIVIDADES DAS CNI 3. O MODELO NORTE-AMERICANO: O TRIBUNAL FISA E A QUEDA DO MURO 4. A "CONSTRUÇÃO PARALELA" E A COMUNICAÇÃO DE INFORMAÇÕES ENTRE AGÊNCIAS 5. CONCLUSÕES 6.

Resumo: A existência de dois tipos de segurança, a nacional e a pública, serviu para habilitar diferentes organismos a preveni-la. Os serviços secretos adquiriram um papel preponderante na segurança nacional, enquanto a segurança pública implica a presença de organismos policiais. Em ambos os casos, o trabalho de vigilância e proteção exige a violação autorizada dos direitos fundamentais. No entanto, o mesmo padrão não existe quando os serviços secretos estão envolvidos, o que é reduzido devido ao facto de não estarem a investigar um ato criminoso e à problemática comunicação das informações obtidas, quando estas aparecem, às forças policiais. Será necessária uma estratégia de ocultação da fonte? Em suma, será necessária uma construção paralela?

Resumen: La existencia de dos tipos de seguridad, la nacional y la pública, ha servido para apoderar a organismos diferentes sobre su prevención. Los servicios secretos han adquirido un protagonismo destacado en lo que respecta a la nacional, mientras que la pública implica la presencia de órganos policiales. Para el trabajo de vigilancia y protección es necesario en ambos casos vulnerar, autorizadamente, los derechos fundamentales. Sin embargo, no existe el mismo estándar cuando participan los servicios secretos que se ve rebajado por no estar investigando un hecho delictivo y la problemática comunicación de la información obtenida, cuando aquel aparece, a las fuerzas policiales ¿Es necesaria una estrategia de ocultación de la fuente? ¿Es precisa, en definitiva, una construcción paralela?

Palavras-chave: Segurança pública, Segurança nacional, Polícia, Serviço de informações, Garantias processuais.

Palabras clave: Seguridad pública, Seguridad nacional, Policía, Servicio de inteligencia, Garantías procesales.

ABREVIATURAS

Art.: Artigo.

CE: Constituição espanhola.

PC: Código Penal.

CESID: Centro Superior de Informação da Defesa.

CIA: Agência Central de Inteligência.

CITCO: Centro de Informação sobre o Terrorismo e a Criminalidade Organizada.

CNI: Centro Nacional de Informações.

DEA: Agência de Controlo da Droga.

DIA: Agência de Informações de Defesa.

MS: Exposição de Motivos.

FBI: Federal Bureau of Investigation.

FJ: Base jurídica.

LOPJ: Lei Orgânica da Magistratura Judicial.

LOPSC: Lei Orgânica de Proteção e Segurança do Cidadão.

LSN: Lei de Segurança Nacional.

NSA: Agência Nacional de Segurança

SAN: Acórdão da Audiência Nacional.

SECED: Serviço Central de Documentação.

SED: Secretário de Estado Diretor.

SIAM: Serviço de Informação de Quadros Superiores.

STC: Acórdão do Tribunal Constitucional.

STS: Acórdão do Supremo Tribunal.

SC: Supremo Tribunal

1. PREFÁCIO.

Desde os atentados às Torres Gémeas de Nova Iorque, em 11 de setembro de 2001 - com as dolorosas réplicas de 11 de março de 2006, em Madrid -, temos vindo a enfrentar um mundo convulsivo, onde os sistemas democráticos se confrontam com várias frentes abertas, desde os conflitos armados à criminalidade organizada transnacional, tendo como pano de fundo riscos terroristas persistentes ou a espionagem levada a cabo por países hostis. Também, de forma menos convencional, temos de estar atentos a ciberataques ou campanhas de desinformação, responder a fluxos migratórios irregulares, a catástrofes climáticas e pandemias globais ou à insegurança económica. Estes factos reflectem um mundo afastado da paz perpétua e expressivo de uma "Sociedade de Risco" que implica o confronto com uma situação de inquietação, não provocada pelas ameaças mas pelos indivíduos que as tornam manifestas (Beck, 2006, p. 107).

Enfrentar os desafios que se colocam, todos eles muito variados, com diferentes raízes e soluções complexas, coloca-nos na esfera da chamada proteção da "Segurança Nacional", um conceito que tem sido explicado a partir de diferentes perspectivas. No entanto, no nosso país, a regulamentação deste conceito é muito recente, com apenas dez anos, e procura dar um enquadramento normativo a um espaço que, tradicionalmente, era colocado na sombra por se considerar que a ação do Estado em determinadas áreas deveria ser mantida em estrito segredo, em claro contraste com a ideia de "Segurança Pública", cuja presença legislativa é muito anterior, obrigatória em democracia, e assenta na ideia de que governar implica o poder de conter o poder de polícia (Zaffaroni, 2006, p. 165).

Em todo o caso, o nosso texto constitucional (doravante CE) não abordou a ideia de "Segurança Nacional", nem contempla uma definição como tal, embora faça alusão ao conceito de "Segurança Pública" em vários preceitos da nossa lex superior ao estabelecer a garantia da "segurança do cidadão" pelas forças policiais (art. 104.1 CE) ou a propriedade exclusiva do Estado sobre a "segurança pública" (art. 149.1.29 CE).¹ CE) ou a titularidade exclusiva do Estado sobre a "segurança pública" (art. 149.1.29^a CE), sem esquecer o art. 126º CE onde se fala de uma "Polícia Judiciária" em situação de dependência dos Juízes e dos Magistrados do Ministério Público na investigação do crime e na descoberta do delinquente (*Cfr.* SSTC 175/1999, de 30 de setembro, FJ 7º 86/2014, de 29 de maio, FJ 4º ou 55/1990, de 28 de março, FJ 5º). Esta situação, de falta de reconhecimento, não impediu que a ideia de "Segurança Nacional" surgisse como um instrumento singular de proteção, como uma política própria, embora sem um ministério para a gerir (Herbon Costas, 2021, p. 164). No entanto, isso não nos impede de observar que ambas as "seguranças" operam nas mesmas esferas, tocam em aspectos semelhantes e estabelecem objectivos idênticos, e embora os direitos fundamentais possam ser violados em ambos os planos, operam sob critérios diferentes, mais flexíveis na sua dimensão ética quando se trata de questões de segurança nacional, e que deixam no ar a existência de uma ponte a ser atravessada em casos de colaboração entre os diferentes órgãos operacionais responsáveis por supervisionar o seu cumprimento.

Do ponto de vista regulamentar, o artigo 3.º da Lei 36/2015, de 28 de setembro, sobre Segurança Nacional (doravante LSN), estabelece que "Para efeitos da presente lei, entende-se por Segurança Nacional a ação do Estado *destinada a proteger a liberdade, os direitos e o bem-estar dos cidadãos, a garantir a defesa de Espanha e dos seus princípios e valores constitucionais*, bem como a contribuir, juntamente com os nossos

parceiros e aliados, para a segurança internacional no cumprimento dos compromissos assumidos". Em consonância com esta definição, a ideia de "Segurança Pública" na Exposição de Motivos (EM) da Lei Orgânica 4/2015, de 30 de março, sobre a Proteção da Segurança Pública (LOPSC) afirma que "A Lei, de acordo com a jurisprudência constitucional, baseia-se num conceito material de segurança pública entendido como uma atividade *destinada a proteger pessoas e bens e a manter a paz de espírito dos cidadãos*, que engloba um conjunto plural e diversificado de acções, diferentes na sua natureza e conteúdo, visando o mesmo objetivo de proteger o bem jurídico assim definido. Dentro deste conjunto de acções estão as acções específicas das organizações instrumentais destinadas a este fim, especialmente as que correspondem às Forças e Corpos de Segurança, a quem o artigo 104º da Constituição *confia a proteção do livre exercício dos direitos e liberdades e a garantia da segurança pública...*".

É facilmente perceptível, como já foi salientado, a ideia comum de proteção de liberdades e direitos que coloca ambos os conceitos num claro fio de ligação, o que pode ser observado até na jurisprudência. Neste sentido, o STC 184/2016, de 3 de novembro, o primeiro acórdão que abordou o conceito de "Segurança Nacional" refere *"Por outro lado, tendo o Estado uma clara competência, quer em matéria de defesa, quer em matéria de segurança pública, não faria sentido que, numa área como a da segurança nacional, tão intimamente ligada a ambas, ao ponto de se identificarem os seus fins e objectivos e os bens jurídicos protegidos nos moldes indicados, a competência do Estado se tornasse meramente residual. Em suma, a segurança nacional não é uma competência nova, mas integra-se nas competências estaduais de defesa e segurança pública"* (FJ 3º). Este acórdão, que mais não faz do que ligar os dois conceitos, não impede que se estabeleçam diferenças claras.

Em primeiro lugar, a defesa da segurança nacional contra ameaças, através da obtenção de informações, é da competência dos serviços secretos, nomeadamente, e no nosso país, do Centro Nacional de Informações (CNI). No caso da segurança pública, ou segurança dos cidadãos, a sua proteção é confiada aos serviços de polícia, sejam eles da administração central, regional ou local. Em segundo lugar, os serviços secretos, na vigilância das actividades susceptíveis de afetar a segurança nacional (espionagem, contraespionagem, luta antiterrorista, etc.), operam sob um critério claro de segurança. Em segundo lugar, as forças de segurança, que desenvolvem a sua atividade sob um claro critério de extrema discricionariedade operacional, pelo que o seu trabalho permanece sob a égide de informação classificada, que não é do conhecimento público, e os resultados do seu trabalho raramente são levados a tribunal, situações que não afectam o trabalho das forças de segurança, que desenvolvem a sua atividade sob a supervisão de órgãos judiciais, com resultados que são públicos e publicitados, sendo o objetivo último conduzir, em regra, à determinação, ou não, de responsabilidade criminal a ser judicialmente elucidada. Em quarto lugar, a violação organizada de direitos fundamentais carece, quer na atividade policial, quer na atividade do CNI, de autorização judicial, embora a moldura processual penal decorrente da Lei de Processo Penal (LECRIM) funcione como flange para os órgãos de segurança pública, os serviços secretos operam num quadro necessariamente mais amplo, em que a regulação normativa é bastante limitada, através do único artigo constante da Lei n.º 2/2002, de 6 de maio, limitando-se a tutela judicial à autorização de medidas que afectem o sigilo das comunicações e de buscas domiciliárias que afectem parcialmente o art. 18.º do Tratado CE, sendo o seu objetivo a recolha de informações cujo destino não é, em princípio, um julgamento. No entanto, várias questões se colocam: como é o nosso modelo de supervisão judicial das

actividades de informações? É possível aos serviços secretos partilharem informações com os organismos policiais? Seria possível utilizá-las no âmbito da investigação criminal e da ação penal? Vejamos diferentes aspectos susceptíveis de formalizar o debate.

2. O MODELO DE AUTORIZAÇÃO JUDICIAL PARA AS ACTIVIDADES DA CNI.

A recolha tradicional de informações por parte dos serviços de espionagem sempre se baseou em técnicas clandestinas e com uma dimensão ética necessariamente flexível no seu desenvolvimento, com um quadro de garantias pouco nítido para os afectados. Quanto maior é a ameaça, mais complexos são os métodos de obtenção de informação, onde a avaliação e a análise se tornam instrumentos de precisão para determinar a resposta, a ação ou a decisão. De facto, a importância dos serviços secretos em democracia reside em ajudar o executivo a seguir linhas específicas na defesa dos interesses nacionais, tornando-se actores importantes na tomada de decisões políticas (Pinto Cebrián, 2019, pp. 51 e ss.). Nada têm a ver com a investigação do facto criminoso, nem do infrator ou da sua perseguição processual (Sánchez Ferro, 2020, pp. 188-189), sem esquecer que é precisamente a segurança nacional que justifica as suas funções e permite a violação, ainda que ordenada, de direitos fundamentais (Aba Catoira, 2020, p. 228).

No nosso país, como antecipei, o CNI, órgão da Administração Geral do Estado de natureza singular (SAN 2632/2009, de 27 de maio, Sala de lo Contencioso (Relator: Gil Ibáñez, FJ 1º), dependente do Executivo e que *"... não é, nem pode ser equiparado a um órgão identificado com uma administração independente, no sentido daquela tipologia de entidades de direito público dotadas da autonomia e independência funcional que as caracteriza: é um órgão instrumental do Governo..."*. *não é, nem pode ser equiparado a um órgão identificado com uma administração independente, no sentido daquela tipologia de entidades de direito público dotada da autonomia e independência funcional que a caracteriza: é um órgão instrumental do Governo..."* (STS 1238/2021, de 18 de outubro, Secção III, (Relator: Conselheiro Requero Ibáñez) FJ 7º), o que reflecte, na sua fisionomia, uma longa evolução na história dos nossos serviços. Assim, sucedeu ao Centro de Informação de Alta Defesa (CESID) que, por sua vez, foi criado pelo Real Decreto 1558/1977, de 4 de julho de 1977, um organismo que reunia os anteriores serviços de informação, o Serviço Central de Informação da Presidência do Governo (CESED) e o Serviço de Informação do Alto Estado Maior (SIAM), Sempre actuou como um órgão de avaliação de informações e, durante os diferentes governos, dependeu do Ministério da Defesa, com exceção de um período de dependência do Ministério da Presidência durante o governo de Mariano Rajoy Brey. A sua integração inicial com membros das Forças Armadas acabou por evoluir com a incorporação de pessoal civil, pelo que este organismo já não pode ser visto como um mero compilador de informações militares face a um potencial conflito militar. O seu trabalho vai mais além, pois as ameaças são cada vez mais heterogêneas, com conflitos assimétricos que se desenvolvem em campos de batalha invisíveis e cuja existência e intervenção é essencial para os enfrentar.

De acordo com o artigo 9.º da Lei 11/2002 de 6 de maio, a CNI é dirigida por um Secretário de Estado (SED), que é a "Autoridade Nacional de Informação e Contra-Informação" com o título de "Diretor", nomeado por Decreto Real sob proposta do Ministério da Defesa, e com um mandato de cinco anos que pode ser sucessivamente prorrogado ou substituído a qualquer momento pelo governo. As suas funções são de

"promoção" e de "coordenação", que se resumem na "direção" das tarefas do organismo, na nomeação dos diferentes cargos de direção, na competência orçamental e na cooperação "com os serviços de informações das Forças e Corpos de Segurança do Estado, e com os órgãos da Administração civil e militar, relevantes para os objectivos das informações...". É coadjuvado por um Secretário-Geral, com a categoria de Subsecretário, a quem compete, entre outras funções, para além de o substituir, "Dirigir o funcionamento dos serviços comuns do Centro através das correspondentes instruções e ordens de serviço" (art. 10º, Lei 11/2002). Estes são, portanto, os principais responsáveis por funções de responsabilidade no CNI, com a possível e hipotética existência da Divisão de Informações Externas, da Divisão de Contra-Informação, da Divisão de Informações Internas, da Divisão de Economia e Tecnologia, juntamente com a Subdireção-Geral de Administração e Serviços e a Subdireção-Geral de Pessoal e um Gabinete de Assessoria Jurídica, um Gabinete Técnico, um Chefe de Apoio Operacional e um Serviço de Segurança (arts. 1 e 2 RD 2632/1985). 1 e 2 RD 2632/1985, de 27 de dezembro de 1985, embora mais tarde, no RD 266/1996, de 16 de fevereiro de 1996, o art. 2.º tenha estabelecido a existência de unidades de informações e de apoio operacional e técnico, juntamente com uma unidade de segurança encarregada de tarefas de proteção). Em todo o caso, é possível que esta organização interna seja atualmente muito diferente.

Entre todas as questões, há uma que se reveste de importância face a uma história que colocou na sombra o trabalho dos nossos serviços secretos. É o caso das actividades de inteligência em que se realizavam buscas e escutas de alvos, cenário órfão de qualquer regulamentação e enormemente problemático até à Lei 2/2002, de 6 de maio, que num único preceito, com impacto através da sua lei transitória sobre a Lei Orgânica do Poder Judicial 6/1985, de 1 de julho (LOPJ), nos arts. 125, 127, 135, juntamente com o novo art. 125, 127, 135, juntamente com o novo art. 342 bis do mesmo texto, decide que um Juiz do Supremo Tribunal (Segunda Secção Penal ou Terceira Secção Administrativa) será responsável por autorizar a CNI a realizar actos que afectem a inviolabilidade do domicílio (art. 18.2 CE) e a interceção de comunicações (art. 18.3 CE). Trata-se de um sistema invulgar (Lanz Muniain, 2023, p.27), sem paralelo nos nossos países vizinhos, com exceção, com relativas nuances, dos Estados Unidos, como veremos, a atribuição de competência a um juiz singular, e por um período temporário de cinco anos, não está isenta de críticas por se afastar do sentido constitucional do juiz ordinário predeterminado por lei (De la Oliva Santos, 2006, p. 154). É evidente que não foi devidamente criado um tribunal de espionagem.

A justificação para a alteração é dada pelo EM da Lei 2/2002 que afirma "Para as actividades que possam afetar a *inviolabilidade do domicílio e o sigilo das comunicações*, a Constituição Espanhola exige, no seu artigo 18.º, autorização judicial, e o artigo 8. 8 da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais exige que essa ingerência esteja prevista na lei e constitua uma medida que, numa sociedade democrática, *seja necessária para a segurança nacional, a segurança pública, o bem-estar económico do país, a manutenção da ordem e a prevenção da criminalidade*, a proteção da saúde ou da moral, ou a *proteção dos direitos e liberdades de outrem*". Como se vê, alude-se às duas seguranças e aos aspectos que as alimentam como elemento justificativo da violação do art. 18º CE e tendo como pano de fundo a proteção dos direitos e liberdades, elemento nuclear de ambas.

O modelo de autorização é extremamente peculiar, regulado no artigo único da Lei n.º 2/2002, de 6 de maio, e em síntese é iniciado pela SED, que submete ao Magistrado do CS (Secção II ou III), eleito pelo Conselho Geral da Magistratura Judicial (CGPJ) por um período de cinco anos - coincidente com o mandato da SED - um pedido de violação de direitos fundamentais, que deve ser devidamente fundamentado e conter necessariamente os seguintes pontos: "a) *Especificação das medidas solicitadas.* b) *Os factos em que se baseia o pedido, os objectivos que o motivam e as razões que aconselham a adoção das medidas solicitadas.* c) *Identificação da pessoa ou pessoas afectadas pelas medidas, se conhecidas, e designação do local onde as medidas devem ser tomadas.* d) *Duração das medidas solicitadas, que não podem exceder vinte e quatro horas no caso da inviolabilidade do domicílio e três meses para a interceção ou interceção de comunicações postais, telegráficas, telefónicas ou de qualquer outro tipo, ambos os prazos prorrogáveis por iguais períodos sucessivos, se necessário.* Recebida a petição apresentada pelo SED, o Juiz do CS dispõe de 72 horas (ou 24 horas consoante a urgência da medida) para acautelar a sua tramitação, que será secreta. A decisão judicial inicial, eventualmente um despacho, e as subsequentes que a prolonguem, não são passíveis de recurso, nem de revisão, e isto porque os únicos intervenientes neste procedimento são o Magistrado do CS e a SED, que, por outro lado, "ordenará a destruição imediata do material relativo a toda a informação que, obtida através da autorização prevista neste artigo, não esteja relacionada com o objeto ou finalidade da autorização".

É evidente que não existem princípios inspiradores do pedido, critérios de deferimento ou indeferimento, utilização ou destino do material obtido, controlo judicial da execução das medidas ou do resultado obtido, com exceção da prorrogação, da situação dos afectados pela medida de imissão ou dos recursos contra a decisão proferida. Neste sentido, a justificação é, a priori, que o material obtido não é suscetível de gerar provas nem será utilizado em processo penal (González Cussac, 2015, p.88). No entanto, não podemos descartar, como primeiro elemento de nuance, a transcendência processual do trabalho de inteligência, como se destaca o uso, na jurisdição contenciosa, dos relatórios da CNI para negar a nacionalidade de requerentes estrangeiros por razões de "segurança nacional" (SSTS 233/2022, 23 de fevereiro, Câmara III, Orador: Sr. Menéndez Pérez, FJ 4º; 395/2022, de 29 de março, da Câmara III, Relator: Sr. Román García FJ 6º; 367/2021, de 17 de março, da Secção III, Relator: Herrero Pina FJ 2º; 4376/2015, de 26 de outubro, da Secção III, Relator: Sr. Del Riego Valledor, FJ 4º; STS 2105/2014, de 26 de maio, da Câmara III, Relator: Sr. Del Riego Valledor, FJ 5º). No entanto, voltarei mais tarde à sua utilização em processos penais para clarificar a questão. Em qualquer caso, o objetivo foi combinar aspectos relativamente antitéticos, como a supervisão de algo que, pela sua própria natureza, não poderia ser supervisionado, abrindo um canal judicial que, por outro lado, não constrange operacionalmente os agentes, mantendo-os fora dos requisitos derivados da existência de um processo penal aberto (Alfonso Rodríguez, 2024, p. 132).

O ponto de partida do pedido gira em torno da alínea b) do artigo 4.º da Lei 11/2002, de 6 de maio, que estabelece, entre outras, como função principal do nosso serviço de espionagem a de "*Prevenir, detetar e permitir a neutralização das actividades de serviços, grupos ou indivíduos estrangeiros que ponham em risco, ameacem ou atentem contra a ordem constitucional, os direitos e liberdades dos cidadãos espanhóis, a soberania, integridade e segurança do Estado, a estabilidade das suas instituições, os interesses económicos nacionais e o bem-estar da população*". Neste sentido, reflecte-se aqui o elemento justificativo do pedido de autorização judicial no artigo único, convertendo o juiz do CS autorizador no intérprete de conceitos não jurídicos como "soberania" ou

"integridade", "interesses económicos nacionais" ou "bem-estar da população", que são os fins últimos do desenvolvimento das tarefas de espionagem e que, juntamente com o respeito pelos direitos, liberdades ou estabilidade institucional, implicam fazer dele o guardião da "segurança nacional" que habilita o serviço a poder desempenhar as suas funções.

A questão levantada pela habilitação judicial da CNI para intercetar um telefone ou entrar numa casa é que ela implica uma espécie de salvaguarda mas afasta-se de uma função de garantia dos direitos fundamentais (Pascual Sarria, 2007, p. 197) que, por outro lado, é atribuída ao Poder Judiciário por força do art. 117.4 CE, e converte o procedimento numa *espécie de processo secreto para solicitar medidas de limitação de direitos fundamentais específicos, no âmbito de operações de inteligência para a proteção da segurança nacional, a um juiz do CS, sujeito a um mandato temporário e expressamente nomeado para o efeito* (Alfonso Rodríguez, 2023, p.89).

3. O MODELO AMERICANO: O TRIBUNAL FISA E A QUEDA DO MURO.

Não é claro se os Estados Unidos foram o modelo para a configuração e fisionomia do nosso sistema de controlo das actividades de informações. Mas é claro que não podemos aceitar uma inspiração total, pois o sistema processual está distante entre os dois países, com o sistema adversarial norte-americano em que as partes (acusador e acusado) são os verdadeiros "donos" do processo penal americano, e onde o princípio do "Due Process of Law", o direito a um processo justo com todas as garantias, se mostra como o "motor" da organização processual (Gómez Colomer, 2006, pp. 50-57), em contraste com um modelo do juiz de instrução que é abençoado por um juiz de julgamento que é o "dono" do sistema (Gómez Colomer, 2006, pp. 50-57), em contraste com o modelo do juiz de instrução que é o "dono" do sistema. 50-57), em contraste com um modelo de juiz de instrução que é abençoado por uma LECRIM de 1882, o que é impossível, em qualquer circunstância, nos Estados Unidos. Note-se, porém, que o modelo processual do Tribunal FISA não responde a este sistema de contraditório.

O modelo de intelligence norte-americano assenta numa pluralidade de agências (CIA, NSA, DIA, FBI no seu ramo de intelligence, Forças Armadas e Departamentos Governamentais com os seus próprios serviços) que passam a ser coordenadas por um Diretor Nacional de Intelligence, de acordo com o Intelligence Reform and Terrorism Prevention Act de 2004 (IRPA), enquanto comissário do Executivo para a adequada coordenação de todas as organizações, coexistindo com um intenso controlo por parte do legislativo através de comissões parlamentares de supervisão. Dada esta circunstância, é necessário partir de uma fase de abusos sistemáticos por parte do FBI ou da CIA, destacados pelo *Comité da Igreja do Senado* (Arrieta, 2025, p. 122). 122), conduziu à promulgação, em 1978, da *Foreign Intelligence Surveillance Act* (FISA), da qual fazia parte a criação de um Tribunal Federal para controlar a vigilância eletrónica de agentes estrangeiros nos Estados Unidos, agora composto por onze juízes federais com identidade pública, mas cujo trabalho é realizado em segredo, e que são nomeados pelo *Presidente do Supremo Tribunal Federal dos Estados Unidos*. São estes juízes que estão encarregados de verificar os pedidos do Executivo, que deve provar como "causa provável" - uma suspeita sensata que motiva o pedido - que o alvo da escuta ou da vigilância dos dispositivos electrónicos é uma potência estrangeira ou um agente de uma potência estrangeira que é alvo da operação de recolha de informações, pelo que a sua utilização não se destinava, a priori, a intercetar as comunicações dos cidadãos

americanos. Na ausência de um caso *prima facie* de infração penal para obter o mandado do Tribunal FISA, o padrão de autorização é menos rigoroso do que o padrão habitual exigido pela aplicação da lei para violar os direitos da quarta emenda - a privacidade (Ruger, 2007, p. 243).

O requerimento é apresentado perante um juiz do Tribunal FISA, no qual o governo comparece com a sua representação como único interveniente processual, onde, para além da prova da causa provável, deve ser indicada a identidade dos envolvidos e dos funcionários envolvidos, a duração das medidas de vigilância eletrónica, certificados das autoridades de inteligência e detalhes de pedidos anteriores, entre outros elementos. O facto de ser o poder executivo a atuar como único participante afasta o procedimento do sistema adversarial típico do sistema norte-americano (Sobel, 2023, p. 15), estimando-se que uma das razões, entre outras avançadas na altura pelo *Procurador-Geral* Griffin Bell durante a elaboração da lei, que poderia motivar a ausência de outros participantes, se deve à relutância do próprio governo em desclassificar informação por receio de fugas de informação (Chin, 2021, p.665).

Perante os dados fornecidos, o juiz da FISA concede, ou nega detalhadamente, o *mandado* de vigilância eletrónica solicitado pelo Governo, identificando os sujeitos, os meios, o tipo de informação a obter e a duração do mandado, podendo a sua recusa ser revista perante o *Tribunal de Revisão da FISA*, composto por três juizes do mesmo órgão, com possibilidade de recurso para o *Supremo Tribunal dos EUA* se a revisão não for bem sucedida.

No entanto, se até 2001 o mandato da FISA servia o propósito da recolha de informações, os ataques terroristas de 11 de setembro nos Estados Unidos, com o *Patriot Act* de 2001, ao abrigo da secção 203, alteraram a arquitetura da lei e, assim, quebraram o *muro* entre a recolha de informações estrangeiras e as investigações criminais (Donohue, 2021, p. 204), permitindo o uso da partilha de informações pelas agências de aplicação da lei (FBI ou DEA), obtidas para efeitos de recolha de informações estrangeiras à luz da FISA, e em investigações criminais, misturando o uso da partilha de informações pelas agências de aplicação da lei (FBI ou DEA), obtidas para efeitos de recolha de informações estrangeiras à luz da FISA, e em investigações criminais. 204), permitindo a utilização da partilha de informações por parte dos serviços responsáveis pela aplicação da lei (FBI ou DEA), obtidas para efeitos de recolha de informações estrangeiras à luz da FISA, e em investigações criminais, misturando assim um método idêntico com finalidades diferentes, o que suscita várias reflexões.

Em primeiro lugar, por força das normas do pedido, na medida em que a credenciação da causa provável é diferente, uma vez que numa investigação criminal era necessário provar, através desse conceito, a possível prática de um ato criminoso, o que não acontece no pedido de um mandado ao abrigo do regulamento FISA. Em segundo lugar, com o objetivo comum de prevenir um ataque terrorista, a cooperação e a transmissão de informações entre as agências de espionagem e as agências de aplicação da lei, cujas tarefas são diferentes, aumentaram e, assim, as fronteiras entre a Comunidade de Inteligência e a agência policial esbateram-se e misturaram-se (Stein, Mondale, Fisher, 2016, p. 2266). Em terceiro lugar, a possibilidade de construir um caso criminal, com informações obtidas de acordo com os critérios da FISA, tornou-se uma possibilidade distinta (pense num caso de terrorismo federal ou narcoterrorismo em que a aplicação da lei recebeu informações de agências de inteligência como resultado dos resultados obtidos

de acordo com um mandado da FISA), de modo que surgiu um debate claro sobre os direitos de devido processo das pessoas afetadas e seu direito de defesa contra a partilha de materiais de inteligência entre agências (Reid, 2015, p. 429).

4. CONSTRUÇÃO PARALELA" E COMUNICAÇÃO DE INFORMAÇÕES ENTRE AGÊNCIAS.

Como resultado do que se observou anteriormente relativamente à queda do muro, é evidente que a "Segurança Nacional", conceito demasiado ambíguo, foi embutida na "Segurança Pública", tendo em conta que os requisitos processuais para a violação de direitos fundamentais, nomeadamente a privacidade das comunicações, foram reduzidos face à pretensão de recolha de informações, informações essas que, mais tarde, fruto de uma mudança de realidades, que levou a uma mutação de princípios, foram utilizadas para diferentes fins, de forma a contornar os costumes processuais e os direitos fundamentais em exercícios de permutabilidade, quer para a tomada de decisões políticas, quer para fundamentar um processo criminal. É neste cenário que faz sentido o conceito de "*construção paralela*", que se iniciou com a receção de informações de inteligência com normas de obtenção aligeiradas, cuja origem não pode ser revelada e que, como já referi, pode pôr em causa garantias processuais, ao proporcionar um atalho operacional que pode contornar objecções legais e que obriga à invenção de um canal paralelo que desvia a atenção da fonte original (e.g. um informador criado artificialmente). Por exemplo, um informador criado artificialmente que oculta informações de inteligência obtidas através de um mandato diferente, como um mandado do Tribunal FISA).

Se anteriormente analisámos o modelo de obtenção de informações por parte da CNI, órgão principal da nossa Comunidade de Informações, a situação enfrentada por um órgão policial, seja ele um órgão estatal como a Polícia Nacional, a Guarda Civil ou o Serviço de Vigilância Aduaneira, ou os casos de Polícias Autónomas, expressivos de um modelo integral (STC 184/2016, de 3 de novembro, FJ 4º) como a Catalunha, Navarra e País Basco, cada uma das quais dispõe de unidades de informação e que constituem uma espécie de "Comunidade de Inteligência Policial" onde intervém o Centro de Inteligência para o Terrorismo e Crime Organizado (CITCO) como órgão de análise e coordenação entre órgãos. No entanto, é de salientar que, em matéria de recolha de informações, as forças policiais estão sujeitas a constrangimentos processuais, no âmbito da satisfação da segurança pública, radicalmente diferentes dos serviços de informações, e onde a autoridade judiciária actua como garante dos direitos fundamentais. Neste sentido, o quadro de atuação previsto na LECRIM condiciona a passagem dos investigadores, sujeitando a sua atividade a um conjunto de princípios e exigências que estabelecem um padrão de garantias processuais inerentes ao Estado de Direito.

Uma investigação criminal pode afetar vários direitos fundamentais, como a liberdade pessoal (art. 17.º CE), a privacidade (art. 18.º, n.º 1 CE), a inviolabilidade do domicílio (art. 18.º, n.º 2 CE), o sigilo das comunicações (art. 18.º, n.º 3 CE) e ainda a liberdade de circulação (art. 19.º CE), determinando a autoridade judiciária, nos pressupostos da lei, a eventual adoção de qualquer medida que afecte os referidos direitos, pelo que, embora deva existir uma autorização legal que permita a sua adoção, tal não é, contudo, suficiente. É necessário que a medida infratora seja suficientemente fundamentada, de modo a expressar a argumentação de facto e de direito que determina a sua adoção, de acordo com os princípios da especialidade, adequação, excecionalidade, necessidade e proporcionalidade. Por outras palavras, deve estar a ser investigada uma

infração penal (especialidade) que, em qualquer caso, deve ser suficientemente grave para justificar a adoção de tal medida, que serve o objetivo da investigação (adequação; SSTC 85/1994, 14 de março, FJ 3º; 181/1995, 11 de dezembro, FJ 5º; 49/1996, 26 de março, FJ 3º; 54/1996, 26 de março, FJ 7º e 8º; 123/1997, 1 de julho, FJ 4º), uma vez que os resultados não podem ser alcançados através de outras medidas menos gravosas para os direitos fundamentais da pessoa investigada, sendo essenciais do ponto de vista do caso concreto (excecionalidade e necessidade) e, por último, só factos graves, socialmente transcendentais e com fortes indícios justificam o sacrifício de direitos fundamentais essenciais sob pena de se assistir a uma situação de impunidade penal (proporcionalidade, STC 49/1999, 5 de abril, FJ 7º).

É evidente que o pedido limitativo de direitos fundamentais que a unidade de polícia instaura para investigar está sujeito aos requisitos justificativos acima referidos, de tal modo que, perante um facto criminoso que está a ser investigado em curso, existe um "muro" que tem de ser ultrapassado por autorização judicial para se poder prosseguir a investigação. Em caso algum se pode fazer uma requisição policial com fins prospectivos (STS 822/2022, 18 de outubro, Câmara II (Relator: Sr. Palomo del Arco) , FJ 1º.3. a)), ou seja, sem um crime prévio indiciariamente justificado, não é sequer concebível a realização de uma requisição destinada a obter uma decisão judicial que viole um direito fundamental. Portanto, é claro que as forças policiais estão lá para investigar sob parâmetros precisos e limitações claras, e embora a clandestinidade da investigação seja precisa, o seu destino final é emergir num julgamento público com pleno respeito pelo direito de defesa e com o objetivo claro de satisfazer as exigências da "segurança pública" (STC 175/1999 de 30 de setembro, FJ 7º ou STC 86/2014, de 29 de maio FJ 4º), algo que contrasta com a tarefa dos serviços secretos onde, no interesse da proteção da "segurança nacional", são recolhidas informações junto de pessoas singulares ou colectivas, nacionais ou estrangeiras, informações essas que são classificadas e que não se destinam certamente a ser publicamente divulgadas junto de um órgão de acusação para deduzir responsabilidades penais e sem que ideias como "contraditório", "defesa", "suspeito" ou "arguido" tenham qualquer substância própria, uma vez que o seu trabalho nada tem a ver com a investigação criminal.

No entanto, apesar do que precede, os campos de ação das forças policiais e dos serviços secretos são comuns. A criminalidade organizada, o terrorismo, a imigração clandestina... constituem uma ameaça simultânea à "segurança pública" e à "segurança nacional", de tal forma que:

A criminalidade organizada é uma ameaça à segurança caracterizada pelo seu objetivo essencialmente económico, pelo seu efeito negativo nas instituições políticas e sociais, pela sua natureza transnacional e pela sua opacidade. Os grupos criminosos e as organizações criminosas disfarçam as suas operações ilegais como negócios legítimos e recorrem cada vez mais a tecnologias digitais, como as criptomoedas e a dark web. Para além da sua dimensão económica, a criminalidade organizada tem um potencial desestabilizador relevante. As suas estruturas adaptam-se ao ambiente geoestratégico e têm impacto na governação, na paz social e no normal funcionamento das instituições. Em termos de criminalidade grave, actividades como a exploração de crianças ou o tráfico para fins de exploração sexual visam grupos vulneráveis e violam gravemente os direitos humanos. O contrabando, a cibercriminalidade, o tráfico de droga, de armas e de animais selvagens e a corrupção constituem ameaças tangíveis à segurança nacional. A convergência entre os grupos terroristas e as redes de criminalidade organizada está a

aumentar. Os padrões organizacionais cada vez mais descentralizados destes actores criminosos favorecem a sua cooperação e facilitam o financiamento do terrorismo (Estratégia de Segurança Nacional (2021), pp. 64-65).

É evidente que, face ao exposto, é necessário que os nossos serviços secretos e as nossas polícias colaborem numa atividade que pode ser materialmente coincidente em termos de factos e de assuntos, daí a sua natureza claramente concêntrica quando se trata, entre outras questões, do terrorismo, da criminalidade organizada ou de ambos. Neste ponto, surge uma dúvida clara: o que acontece quando a CNI, em resultado das suas escutas, tem conhecimento de um ato criminoso que pode ser investigado devido à sua iminência?

É evidente a inexistência de um sistema de vasos comunicantes legalmente regulamentado para formalizar a transmissão de informações quando a CNI toma conhecimento da prática de actos criminosos (Sánchez Barrilao, 2011, p. 61), uma vez que quase não existem referências na Lei n.º 11/2002, de 6 de maio, relativamente à cooperação com as Forças de Segurança, exceto em aspectos específicos como o art.º, n.º 2, alínea d), que atribui à SED a manutenção e desenvolvimento da "colaboração com os serviços de informações das Forças e Corpos de Segurança do Estado e com os órgãos da administração civil e militar, relevantes para os objectivos de informações". É aqui que entra em cena o que anteriormente apontámos como "*construção paralela*" como expressão da configuração de um processo criminal por uma força policial ocultando a origem da fonte que o move (Reid, 2015, p. 427) e que poderá estar necessariamente ligada a informações obtidas por uma agência de intelligence, tendo que construir elementos de prova circunstanciais paralelos que pretendem ser o manto que esconde a génese da informação original, o que nos obriga a ver como devemos tratar o material de intelligence como iniciador ou impulsionador de uma investigação policial criminal.

Em princípio, é necessário partir do que é afirmado no STS 746/2022, de 21 de julho, Câmara II, (Relatora: Polo García) que assinala

"Como dissemos no acórdão citado pela Câmara - 312/2021, de 13 de abril - não há direito dos arguidos a revelar o conteúdo e o alcance das colaborações policiais internacionais. *Os investigados sujeitos a processo penal não têm o direito de revelar os pontos de destacamento policial, nem a identidade dos informadores, nem as informações recolhidas através de técnicas criminalísticas que perderiam a sua eficácia se fossem massivamente divulgadas. Não existe o direito de conhecer os instrumentos e materiais específicos de que a polícia dispunha para a investigação e que poderiam tornar-se ineficazes para futuras intervenções.* Também não existe o direito de conhecer as investigações de outros crimes que possam ser imputados aos mesmos suspeitos, mas que ainda se encontram em fase de confirmação policial, menos ainda se considerarmos que, se for caso disso, devem ser objeto de um processo penal autónomo (art. 17.º, n.º 1, da LECRIM). É também inaceitável que se conheçam investigações que nem sequer afectam os processados e que podem arruinar outras acções policiais de obrigatória perseguição criminal". (FJ 3.3).

A origem da decisão anterior deveu-se à recusa do órgão judicial responsável pela acusação em aceitar o testemunho de agentes americanos da DEA que forneceram

informações à Polícia Nacional que efectuou uma investigação sobre drogas que culminou numa condenação. Note-se que a decisão anterior não era nova; o nosso Tribunal Superior já tinha deixado claro que "...quando os serviços de inteligência estrangeiros fornecem dados às forças e órgãos de segurança espanhóis, o requisito de que a fonte de conhecimento também precisa das suas próprias fontes de conhecimento não faz parte do conteúdo do direito a um julgamento com todas as garantias..." (STS 445/2014, de 29 de maio, Câmara II, Relatora: Sra. Ferrer García FJ 2º ; STS 884/2012, de 12 de novembro, da Câmara II, Relator: Sr. Marchena Gómez FJ 8). Obtemos, assim, uma primeira solução parcial: os serviços de informações estrangeiros podem fornecer às nossas forças policiais as suas fontes sem qualquer problema para iniciar a investigação. A sua origem, em suma, não é relevante e, por conseguinte, a DEA (ou o FBI, ou qualquer outra força policial estrangeira) poderia receber informações da sua própria agência de informações (CIA, NSA... ou o seu serviço de informações) e transmiti-las às agências policiais para iniciar um processo penal no nosso país, sem entrar no debate sobre a flexibilização das normas legais para a sua obtenção, uma vez que não há direito a debater as fontes da informação, dado que não é necessário conhecê-las para instaurar um processo justo.

A questão da transmissão às forças de segurança, pelo CNI, das informações que conseguiu obter em resultado das suas escutas telefónicas ou buscas domiciliárias carece de maior esclarecimento e é, de facto, matéria abordada na jurisprudência que nega que as suas funções tenham qualquer relação com a investigação criminal (SSTS 1140/2010, de 29 de dezembro, da Câmara II (Relator: Berdugo Gómez de la Torre); 1094/2010, de 10 de dezembro, da Câmara II (Relator: Marchena Gómez)). E sobre este ponto, mais uma vez, a diferente metodologia processual exigida para uma interceção telefónica, por exemplo, consoante seja solicitada pelo CNI ou por um órgão policial, é que apenas têm em comum a necessidade de autorização judicial, nada mais.

Não faltam argumentos a favor do facto de as informações obtidas pelo CNI em violação de um direito fundamental, e nas suas próprias condições processuais - não processuais -, com autorização judicial, poderem servir de fonte para o início de um processo penal com a eventual comunicação às forças policiais.

Em primeiro lugar, existe *um princípio de unidade de ação entre a polícia e os serviços de informações*, imposto pelas Estratégias Nacionais de Segurança que são ditadas como quadro de ação (art. 4.3 LSN). Assim:

Nos domínios tradicionais da segurança, a adaptação à natureza evolutiva das ameaças - conflitos armados, terrorismo, criminalidade organizada, proliferação, fluxos migratórios irregulares, actividades de informação - é uma constante na *ação dos diferentes intervenientes na segurança nacional*. medida que estes fenómenos se tornam cada vez mais transnacionais, *intensifica-se a necessidade de uma ação concertada* a todos os níveis. As ligações estreitas que existem frequentemente entre várias destas ameaças tornam necessário abordá-las a partir de quadros estratégicos e operacionais alargados, com *base no princípio da unidade de ação*. Este relatório mostra que esta abordagem já é plenamente válida na resposta de Espanha aos desafios clássicos de segurança (Estrategia de Seguridad Nacional, 2013, p. 145).

É difícil, sob pena de pôr em perigo a comunidade, admitir trabalhos configurados em compartimentos estanques, pelo que a LSN impõe esta "unidade de ação" (art. 4.º, n.º

2), lembrando no art. 9.º, n.º 2 que "Os *Serviços de Informações e Inteligência do Estado*, no âmbito das suas competências, apoiarão permanentemente o Sistema de Segurança Nacional, fornecendo elementos de julgamento, informações, análises, estudos e propostas necessários para prevenir e detetar riscos e ameaças e *contribuir para a sua neutralização*". Por conseguinte, a exigência de um sentido convergente traduz-se necessariamente na cooperação entre organismos ("Serviços") para o cumprimento dos requisitos destinados a prevenir riscos ("contribuir para a sua neutralização"). Em suma, a comunicação de informações é um elemento-chave para ajudar a neutralizar os riscos que surgem.

Em segundo lugar, a justificação da comunicação pode ser dada pela *obrigação de denunciar os factos criminosos ou a sua iminente prática* por quem os testemunhe, nos termos do art. 262.º da LECRIM (De la Oliva Santos 2006, p. 164), a começar pelo magistrado do CS que autorizou a interceção das comunicações ou a entrada no domicílio do CNI (López Alafranca, 2014, p. 135). 164) a partir do magistrado do CS que autorizou a interceção de comunicações ou a entrada no domicílio da CNI (López Alafranca, 2014, p. 135) e também por força da exigência de responsabilidade criminal (407 e 408 CP) quando estamos a falar de polícias que podem prestar serviços à CNI. O conhecimento do juiz sobre o desenvolvimento da medida autorizada tem necessariamente de derivar da necessidade de prorrogação das medidas limitativas de direitos fundamentais que possam interessar à CNI, pois não há possibilidade de o órgão autorizador desconhecer os factos, a não ser que se admita uma autorização "cega", como um "cheque em branco" e sem controlo sucessivo, o que não é possível, pois a lei prevê essa prorrogação "em caso de necessidade" (art. 2 d) Lei 2/2002), necessidade essa que teria de ser justificada, com os factos resultantes da medida inicialmente acordada, para a continuação das medidas restritivas.

Não se pode aceitar a tese, sem prejuízo da sua validade, de que a não consideração dos agentes da CNI como autoridades (art. 5.º, n.º 4, da Lei n.º 11/2002) impede a obrigação de denunciar os crimes (Lanz Muniain, 2023, p. 34), no entanto, a obrigação imposta pelo art. 262.º da LECRIM a quem "em razão dos seus cargos, profissões ou ofícios" tenha conhecimento do facto criminoso determina que é indiferente ser ou não uma autoridade ou um seu agente, pois tem conhecimento do facto através da sua profissão e deve denunciá-lo. No entanto, esta comunicação foi subscrita pelo próprio CS quando afirma que "Portanto, a função legal deste Serviço não é a investigação de crimes específicos, sem prejuízo do facto de que, se no decurso do seu trabalho *descobrirem* ou tiverem indícios de acções criminosas, *informam os órgãos policiais e judiciais competentes*, mas - insiste-se - a sua atividade não visa diretamente a descoberta de crimes, nem está condicionada à prévia prática de qualquer" (STS 1140/2010, de 29 de dezembro, da Câmara II (Relator: Berdugo Gómez Gómez). Berdugo Gómez de la Torre) FJ 9º) .

Em terceiro lugar, *uma hipotética classificação secreta não pode cobrir a impunidade de actos criminosos* (López Alafranca, 2014, p. 136), que, por outro lado, devem necessariamente ser evitados. De igual modo, mesmo quando se trate de informação classificada ("organização e estrutura interna, meios e procedimentos, pessoal, instalações, bases de dados e centros de dados, fontes de informação e informações ou dados que possam conduzir ao conhecimento das matérias acima referidas..." ex art. 5.1 da Lei 11/2002), nada obsta a um procedimento de desclassificação de informação a nível processual, mas esta é uma questão alheia à própria comunicação que, precisamente, tem como limite a informação transmitida em que não se divulgue

matéria que deva ser desclassificada (Pascual Sarria, 2007 p. 214).

Em quarto lugar, é precisamente a recolha de informações pelo CNI, se implicar uma violação da privacidade das comunicações ou uma entrada no domicílio, *que é apoiada por uma decisão judicial necessariamente motivada pelo seu efeito prejudicial* (SSTC 126/1995, 25 de julho, FJ 2; 139/1999, 22 de julho, FJ 2; no mesmo sentido, SSTC 290/1994, 27 de outubro, FJ 31; 50/1995, 23 de fevereiro, FJ 5; 41/1998, 23 de fevereiro, FJ 34; 171/1999, 23 de setembro, FJ 10; 8/2000, 8 de janeiro, FJ 4); 41/1998, de 24 de fevereiro, FJ 34; 171/1999, de 27 de setembro, FJ 10; 8/2000, de 17 de janeiro, FJ 4), pelo que tais medidas não foram acordadas fora de um esquema processual ou por capricho, de acordo com as suas necessidades operacionais, pelo que não há ilegalidade na sua obtenção e, portanto, nem na sua comunicação para o início de uma investigação criminal, investigação essa que não está contaminada.

A este respeito, há que distinguir o aspeto probatório da questão propriamente dita da comunicação para a instauração do processo penal. Trata-se de questões diferentes. O material obtido pela CNI não se destina a constituir prova em processo penal, e isto porque é o próprio inquérito policial que se destina a cumprir essa função, recordando que só existe "prova ilícita" (art. 11.º da LOPJ) "quando os meios utilizados para a sua obtenção forem constitucionalmente ilegítimos" (STC 49/1999, de 5 de abril, FJ 12). Neste sentido, o STS 1094/2010, de 10 de dezembro, na sua FJ 2 A recorda-nos que ".... Mas o que é indubitável é que a existência de um processo penal subsequente em que a *notitia criminis* não seja alheia ao ficheiro de segurança processado pela CNI não implica a transmutação da funcionalidade desse ficheiro, que deixaria de ser o que é, distanciando-se dos seus princípios reguladores, para passar a ser um ato processual sine qua non do processo real e, portanto, sujeito às regras gerais que regem o princípio da publicidade".

E é precisamente a decisão judicial autorizadora que nos impede de falar de uma espécie de "parapeito" ilegal por onde o nosso serviço de informações se deslocaria arriscadamente. No entanto, embora tenhamos dito que o material dos serviços de informações não se destina ao processo penal como elemento de prova, não se deve esquecer que "E no que respeita à incorporação no processo de elementos de prova obtidos pelos serviços de informações e que se referem a material desclassificado, ela pode ser apreciada sob duas perspectivas diferentes. Ou actua no processo penal como prova documental, quando se trata de uma prova com estas características, ou serve para conduzir a investigação penal através do depoimento das testemunhas dos autores" (STS 1140/2010, de 29 de dezembro, Câmara II (Relator: Berdugo Gómez de la Torre) FJ 9º).

No entanto, não faltam objecções ao sistema, a começar pelas complexidades que a presença dos serviços secretos no processo penal poderia acarretar (Hassemer, 2000, p. 114), de modo que poderia haver uma confusão, quase uma mistura, que tornaria indistinguíveis as funções de polícia e de recolha de informações (Orgis, 2011, p. 162). Não seria bom para as forças policiais, não seria bom para os serviços secretos, e isto em virtude dos diferentes parâmetros de atuação. Por outro lado, a obtenção de uma escuta telefónica ou de uma entrada domiciliária pelos nossos serviços secretos está sujeita a um padrão diferente, em que é preciso justificar os próprios extremos de perigo para a segurança nacional que podem não ter nada a ver com a prática de um ato criminoso. Em suma, uma coisa é a descoberta, no decurso de uma operação de informações, de um ato criminoso grave ou cuja prática está iminente, o que tem necessariamente de ser

comunicado ou reportado às forças policiais, e outra bem diferente é o procedimento de pedido e obtenção de uma escuta telefônica ou de uma entrada no domicílio pelos serviços secretos servir, como atalho processual, para a busca do próprio crime, o que levaria à irrelevância do sistema de garantias processuais constitucionais no que respeita à limitação e à violação de direitos fundamentais.

Por último, referimos anteriormente que nem toda a informação pode ser conhecida, o que pode levar, no âmbito de um processo penal, a que o direito de defesa seja posto à prova (art. 24.º, n.º 2, CE), uma vez que o acesso ao processo, no caso da CNI, está sujeito a restrições e a uma situação de classificação que contrasta com a disponibilização às partes envolvidas de todos os elementos da investigação criminal. Por outras palavras, a presença dos serviços secretos e as informações por eles obtidas no âmbito do processo penal não podem surgir tão naturalmente como num inquérito policial. Em suma, nem todos têm acesso a todas as informações, o que significa que há elementos que não são objeto de uma hipotética estratégia de defesa, quer de um investigado, quer de terceiros alheios ao processo cujas comunicações ou endereços possam ser afectados, que permanecerão ocultos, o que pode servir para pôr em causa a pureza do processo e da decisão sobre a responsabilidade penal.

5. CONCLUSÕES.

Existe uma relação concêntrica entre a segurança nacional e a segurança pública, na medida em que ambas funcionam com base no pressuposto da existência de ameaças ao Estado de direito. No entanto, os actores com poderes para as proteger são diferentes, tendo os serviços secretos jurisdição sobre a primeira e a polícia sobre a segunda. Neste sentido, foram criados instrumentos para evitar os riscos acima referidos através da atribuição de medidas de limitação dos direitos fundamentais. No caso dos organismos de segurança pública (polícia estadual, regional ou local), as suas competências estão enquadradas no âmbito do processo penal com orientações muito rigorosas para a violação de direitos através da necessidade de autorização judicial para autorizar actividades invasivas mas ordenadas das forças de segurança no quadro do LECRIM. Os serviços de informações (CNI) só há relativamente pouco tempo foram habilitados a interceptar comunicações e a entrar em domicílios através de uma lei de controlo judicial de 2002, mas não podemos afirmar que os seus requisitos coincidam com os da LECRIM para a sua concessão, pelo que nos encontramos perante um sistema de dois pesos e duas medidas consoante o sujeito que actua.

O conceito de *construção paralela* resulta de uma forma de atuação das forças policiais que recebem informações de intelligence que, por um lado, lhes permitem construir processos criminais, mas que, por outro, tendo em conta que existe um padrão mais baixo para a obtenção de informações de intelligence, são obrigadas a ocultar a sua origem, procurando procedimentos alternativos para evitar que a fonte original venha à tona e permitindo que o investigado questione a sua aquisição, violando o devido processo legal. Esta questão surgiu sobretudo na América do Norte, na sequência da queda do "muro" entre a polícia e as actividades de intelligence com os atentados de 11 de setembro de 2001, o que suscitou dúvidas sobre a utilização de informações obtidas através do Foreign Intelligence Surveillance Court (FISA Court), cujos mandados de vigilância a uma agência de intelligence fornecem informações que podem depois ser utilizadas pelas forças policiais, que puderam evitar ter de justificar uma causa provável perante um órgão judicial para levar a cabo as suas investigações. Por outras palavras, parece ser uma

espécie de atalho operacional que gera dúvidas, dúvidas que também nos afectam sobre a possível utilização de informações resultantes de uma autorização do juiz do CS à CNI fora de uma escuta telefónica, fora de uma entrada domiciliária. Neste sentido, há uma série de requisitos que motivariam a comunicação de um facto criminoso resultante da prática de um procedimento restritivo de direitos fundamentais por parte dos nossos serviços secretos aos órgãos policiais, que bem poderia ser a obrigação geral de comunicação prevista no art. 262º da LECRIM. Mas uma elementar unidade de ação na prevenção de ameaças que afectam conjuntamente a segurança pública e nacional exige a cooperação entre serviços e a partilha de informações. Ninguém duvida da necessidade de comunicação e alerta, independentemente da eventual classificação secreta da informação, classificação essa que não pode encobrir o silêncio perante um acto criminoso ou permitir a sua impunidade. Existe também um processo de desclassificação para o efeito.

O nosso CS afirmou que, quando um serviço de informações estrangeiro envia uma confidência que serve para abrir um processo penal, não há direito a conhecer a fonte da mesma, pelo que não é necessário, nem adequado, ocultar a origem ou fonte de conhecimento por parte do órgão policial. No caso da comunicação pelo CNI a uma força de segurança pública, o nosso Tribunal Superior também aprova, ainda que isoladamente, a comunicação de um facto criminoso sem entrar na questão de saber se a informação é ou não classificada como secreta, o que significa que não parece fazer sentido nem a ocultação nem o desenvolvimento de estratégias alternativas, que possam comprometer o processo penal. Não há, pois, lugar a *construções paralelas*, sem prejuízo de a presença dos serviços secretos no processo penal suscitar questões que, a serem resolvidas, exigirão uma reforma do sistema desenhado pela Lei n.º 2/2002, de 6 de maio.

6. REFERÊNCIAS BIBLIOGRÁFICAS.

- Aba Catoira, A. (2020). Responsabilidade e serviços de inteligência. Em J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Tirant lo Blanch.
- Alfonso Rodríguez, A. J. (2023). Governança democrática e responsabilidade: controle judicial das atividades de inteligência (ODS 16.6). *Revista de Derecho UNED*, (31).
- Alfonso Rodríguez, A. J. (2024). Interceção de comunicações telefônicas, segurança(s) e garantias processuais. *Revista Ciencia Policial*, (182).
- Arrieta, G. (2025). Balancing the scales: Amici curiae as special masters in the shadow of FISA [Equilibrando a balança: Amici curiae como mestres especiais à sombra da FISA]. *California Western Law Review*, 61(1), Artigo 6. <https://scholarlycommons.law.cwsl.edu/cwlr/vol61/iss1/6>
- Beck, U. (2006). *La sociedad del riesgo: Hacia una nueva modernidad*. Paidós Ibérica.
- Chin, S. (2021). Introduzindo a independência no Tribunal de Vigilância de Inteligência Estrangeira. *The Yale Law Journal*, 131(2). <http://www.yalelawjournal.org/author/simon-chin>
- De la Oliva Santos, A. (2006). *Escritos sobre direito, justiça e liberdade*. Editorial UNAM, Instituto de Investigaciones Jurídicas.
- Donohue, L. K. (2021). A evolução e a jurisprudência do Tribunal de Vigilância de Informações Externas e do Tribunal de Revisão de Informações Externas. *Harvard National Security Journal*, 12.
- Gómez Colomer, J. L. (2006). Sistema adversarial, processo acusatório e princípio acusatório: Uma reflexão sobre o modelo de persecução penal aplicado nos Estados Unidos da América. *Revista Poder Judicial*, (Especial XIX).
- Hassemer, W. (2000), Processo penal sem proteção de dados? Em C. M. Romeo Casabona (Ed.), *La insostenible situación del derecho penal* (pp. 103-128). Comares.
- Herbón Costas, J. J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional: La pandemia por covid-19 y la necesidad de una urgente reforma. *Revista Española de Derecho Constitucional*, 121. <https://doi.org/10.18042/cepc/redc.121.05>
- Lanz Muniain, V. (2023). El CNI un servicio de inteligencia y seguridad: Panorama normativo. *Revista Española de Derecho Militar*, (119).
- López Alafranca, M. (2014): Mas quem vigiará os vigilantes? *Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (92).

- Orgis, M. (2011). Intelligence-led and intelligence-guided operations: The best option for combating pre-eminent threats. In J. Fernández Rodríguez, D. Sanso-Rubert Pascual, J. Pulido Grajera, and R. Monsalve (Eds.), *Intelligence issues in contemporary society* (pp. 143-166). Ministério da Defesa.
- Pascual Sarria, F. (2007). El control judicial a la interceptación de las comunicaciones: Especial referencia al control judicial previo a las intervenciones del Centro Nacional de Inteligencia. *Revista Española de Derecho Militar*, (89).
- Pinto Cebrián, F. (2019). *Manual de inteligência e contra-inteligência (terrorismo e contraterrorismo)*. Amabar.
- Reid, L. (2015). Partilha de informações da NSA e da DEA: Porque é legal e porque é que a Reuters e a Good Wife se enganaram. *SMU Law Review*, 68(2), Artigo 5.
- Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court: An empirical perspective [As nomeações do Presidente do Supremo Tribunal Rehnquist para o Tribunal FISA: Uma perspectiva empírica]. *Northwestern University Law Review*, 101(1).
- Sánchez Barrilao, J. F. (2011). Prevenção e inteligência: o Centro Nacional de Inteligência e a comunidade de inteligência frente ao terrorismo, ao crime organizado e à imigração ilegal. *Revista Ejército*, (846).
- Sánchez Ferro, S. (2020). Missão impossível? Uma tentativa de compreensão jurídica do mundo da espionagem em Espanha. Em J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 159-207). Tirant lo Blanch.
- Sobel, A. X. (2023). Protecções processuais num tribunal secreto: os amici da FISA e a expansão da revisão de recurso das decisões da FISA. *University of Pennsylvania Law Review*, 172 [Nota: Corrigido "Pennsylvania" para "Pennsylvania". Faltam os números das páginas ou o número do artigo].
- Stein, R., Mondale, W., & Fisher, C. (2016). No longer a neutral magistrate: The Foreign Intelligence Surveillance Court in the wake of the war on terror. *Minnesota Law Review*, 100. https://scholarship.law.umn.edu/faculty_articles/564
- Zaffaroni, E. R. (2006). *El enemigo en el Derecho Penal*. Dykinson.



II.- TRABALHOS DE INVESTIGAÇÃO



Artigo de investigação

A ESPANHA FACE À DESINFORMAÇÃO: DESAFIOS HÍBRIDOS E RESPOSTAS CONVENCIONAIS

Tradução para o português com ajuda de IA (DeepL)

Juan Francisco Adame Hernández

Diretor de Estratégia, Comunicação e Promoção da Casa Árabe

Mestrado em Gestão Sénior de Segurança Internacional

Mestrado em Estudos Avançados em Comunicação Política

juanfcoadame@gmail.com

Recebido a 08/04/2025

Aceite em 03/06/2025

Publicado em 27/06/2025

Citação recomendada: Adame, J. F. (2025). Espanha face à desinformação: desafios híbridos e respostas convencionais. *Revista Logos Guardia Civil*, 3(2), pp. 37-70.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

A ESPANHA FACE À DESINFORMAÇÃO: DESAFIOS HÍBRIDOS E RESPOSTAS CONVENCIONAIS

Resumo: INTRODUÇÃO. 2. DESINFORMAÇÃO, PÓS-VERDADE E NOTÍCIAS FALSAS. 2.1. Conceitos e definições. 3. ESTRATÉGIAS HÍBRIDAS E ZONA CINZENTA. 3.1 Manipulação e interferência de informação estrangeira (FIMI). 4. DOMINÂNCIA COGNITIVA E DESINFORMAÇÃO. 5. CONSTRUÇÃO DE NARRATIVAS E ENQUADRAMENTOS. 5.1. Implementação. 5.2. Impacto das Narrativas e Frames no Domínio Cognitivo. 6. EVOLUÇÃO DA DESINFORMAÇÃO. 7. MEDIDAS E FERRAMENTAS ACTUAIS PARA COMBATER A DESINFORMAÇÃO EM ESPANHA. 7.1. Procedimento de Ação contra a Desinformação. 8 CONCLUSÕES. 9 REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: No atual ambiente geopolítico, caracterizado pela proliferação das tecnologias de informação e pela interconexão global, **a desinformação estabeleceu-se como uma ameaça multidimensional** que compromete as estruturas de segurança nacional e a coesão social dos Estados. Este artigo analisa **a resposta institucional e estratégica de Espanha à desinformação**, enquadrando-a no contexto mais vasto das estratégias híbridas e da **interferência e manipulação de informação estrangeira (FIMI)**.

O estudo aborda conceitos-chave como a *desinformação*, a *pós-verdade* e a *zona cinzenta*, relacionando-os com a **evolução doutrinária das estratégias híbridas na União Europeia**. É dada especial atenção ao **domínio cognitivo** e aos mecanismos de construção de narrativas e quadros interpretativos utilizados para moldar e distorcer a perceção pública. A secção final oferece uma **avaliação crítica das principais medidas adoptadas pela Espanha para combater a desinformação**, avaliando a sua coerência, implementação e eficácia num cenário de ameaça em constante mudança.

Resumen: En el actual entorno geopolítico, caracterizado por la proliferación de tecnologías de la información y la interconexión global, **la desinformación se ha consolidado como una amenaza multidimensional** que compromete las estructuras de seguridad nacional y la cohesión social de los Estados. Este artículo analiza **la respuesta institucional y estratégica de España frente a la desinformación**, enmarcándola dentro del contexto más amplio de las estrategias híbridas y de la **interferencia y manipulación informativa extranjera (FIMI)**.

El estudio aborda conceptos clave como *desinformación*, *posverdad* y *zona gris*, vinculándolos con la **evolución doctrinal de las estrategias híbridas en el seno de la Unión Europea**. Se presta especial atención al **dominio cognitivo** y a los mecanismos de construcción de narrativas y marcos interpretativos empleados para moldear y distorsionar la percepción pública. La última sección ofrece una **evaluación crítica de las principales medidas adoptadas por España para contrarrestar la desinformación**, valorando su coherencia, aplicación y eficacia en un panorama de amenazas en constante transformación.

Palavras-chave: Desinformação, *Notícias falsas*, Estratégias híbridas, Domínio cognitivo, Narrativas.

Palabras clave: Desinformación, *Fake news*, Estrategias híbridas, Dominio cognitivo, Narrativas.

ABREVIATURAS

CIS: Centro de Investigações Sociológicas

CNI: Centro Nacional de Informações

DESI: Índice de Economia e Sociedade Digital

DHS: Departamento de Segurança Interna

SEAE: Serviço Europeu para a Ação Externa

ELISA: Estudo simplificado de fonte aberta

ENISA: União Europeia para a Cibersegurança

ESN: Estratégia de Segurança Nacional

UE/UE: União Europeia

FIMI: Manipulação e interferência de informações estrangeiras

IFJ: Federação Internacional de Jornalistas

INCIBE: Instituto Nacional de Cibersegurança é a cibersegurança.

MAEUEC: Ministério dos Negócios Estrangeiros, da União Europeia e da Cooperação

MPJRC: Ministério da Presidência, da Justiça e das Relações com os Tribunais

OMS: Organização Mundial de Saúde

NATO/NATO: Organização do Tratado do Atlântico Norte/Organização do Tratado do Atlântico Norte

1. INTRODUÇÃO

Na atual era digital, marcada pela rápida disseminação de informação através das redes sociais e das tecnologias de comunicação, a desinformação tornou-se uma importante ameaça estratégica. Este fenómeno, que inclui *as fake news* e a pós-verdade, adquiriu uma relevância sem precedentes na esfera geopolítica, afectando tanto a estabilidade dos sistemas políticos como a perceção pública e a segurança nacional. A Espanha não ficou imune a estes desafios, enfrentando campanhas de desinformação que, em muitos casos, foram utilizadas como ferramentas no âmbito de estratégias híbridas mais amplas.

A desinformação é frequentemente interpretada como um fenómeno em si mesmo ou abordada de forma isolada ou descontextualizada (Lazer et al., 2018). As estratégias em que a desinformação está inserida são relativizadas, abstraídas ou ignoradas (MAEUEC, 2021). Obviando a necessária abordagem multidisciplinar (Wardle e Derakhshan, 2017) ou a necessidade de identificar os objetivos estratégicos que essas ações ou campanhas de desinformação perseguem (Terán, 2019). Mesmo quando há uma referência a estratégias híbridas e/ou à zona cinzenta, geralmente não é abordada em profundidade, sendo relegada a uma mera menção (DSN, 2021). A desinformação, longe de ser um fenómeno isolado, faz parte de um quadro estratégico mais amplo, incluindo estratégias híbridas e a chamada "zona cinzenta" (NATO, 2024) e, especialmente, a *Manipulação e Interferência de Informação Estrangeira* (FIMI).

2. DESINFORMAÇÃO, PÓS-VERDADE E NOTÍCIAS FALSAS

A desinformação não é um fenómeno recente (Allcott e Gentzkow, 2017; Tandoc, Lim & Ling, 2018). Desde que as sociedades começaram a organizar-se em estruturas hierárquicas, os seres humanos têm fabricado e disseminado deliberadamente histórias incorrectas e enganosas (Burkhardt, 2017). Desde as táticas de difamação política na Roma Antiga até às estratégias de propaganda durante a Primeira e a Segunda Guerras Mundiais (Posetti e Matthews, 2018), a desinformação tem sido utilizada para manipular e convencer os outros. A desinformação atingiu níveis sem precedentes, alterando não só a perceção pública, mas também influenciando diretamente os processos políticos e sociais a nível mundial. No entanto, como Julie Posetti e Alice Matthews analisam na sua compilação *"A Short Guide to History of Fake News and Disinformation"* (2018), a fabricação e manipulação de informação não é um fenómeno novo.

Nos últimos anos, os media, as campanhas políticas ou os debates desportivos (ou não desportivos) nas redes sociais têm sido preenchidos com novos conceitos como *fake news* (Tandoc, Lim & Ling, 2018), *post-truth* (McIntyre, 2018) ou *disinformation/misinformation* (Comissão Europeia, 2022). Ganhou relevância pública devido a uma série de eventos internacionais, como o que aconteceu com o Campeonato do Mundo no Qatar (Newtral, 2022), o escândalo da Cambridge Analytica (Chan, 2020) ou o que aconteceu nas eleições presidenciais dos EUA (BBC World, 2018); o que reacendeu o debate sobre as suas implicações nos sistemas democráticos, na perceção pública e nos interesses geopolíticos de determinados países. Trata-se de um debate recorrente, onde o papel das redes sociais, dos media tradicionais, dos verificadores ou da cibersegurança são frequentemente destacados. Esta realidade polissémica, confusa e muitas vezes ambígua reúne diferentes conceitos que tentam nomear, explicar ou aludir a diferentes realidades.

2.1. CONCEITOS E DEFINIÇÕES

Desinformação, *fake news* ou pós-verdade são termos, palavras e conceitos que se tornaram muito populares, passando a fazer parte do discurso coloquial e sendo muitas vezes utilizados como sinónimos, numa tentativa de refletir uma realidade que é normalmente diferente e complexa. No entanto, embora estes termos sejam muitas vezes utilizados indistintamente, cada um deles tem nuances e características específicas que os distinguem, o que é crucial para uma compreensão mais profunda do fenómeno (DSN, 2022).

Quadro 1		
Conceito	Definição	Relação com a verdade
Notícias falsas	Notícias inventadas sem qualquer base factual	Completamente falso
Pós-verdade	Quando as emoções são mais importantes do que os factos	O emocional tem precedência sobre o real
Desinformação	Informações falsas ou manipuladas divulgadas deliberadamente para fins estratégicos	Mistura verdades e falsidades para gerar um efeito concreto.

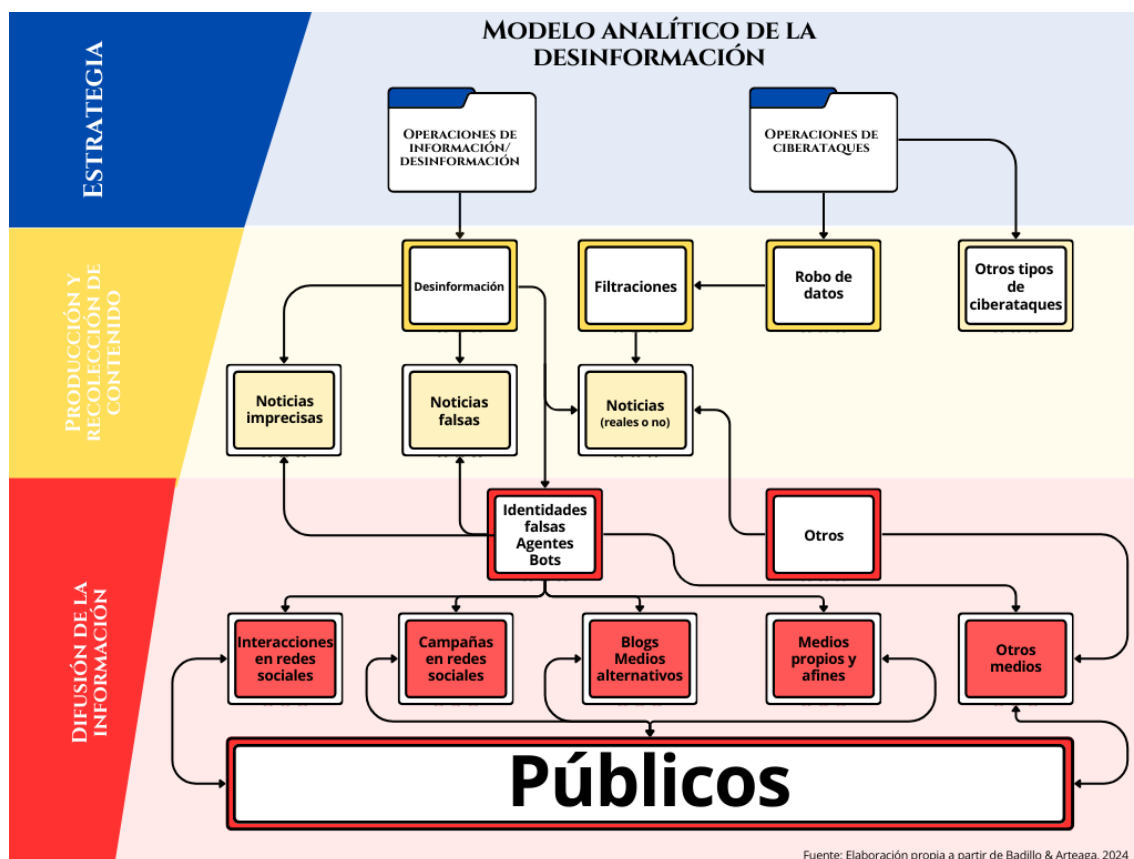
Fonte: Elaboração própria

Comecemos por desvendar esta complexa miscelânea de temas pelo aspeto mais simples, *as fake news*. Entendemos por *notícias falsas* as notícias falsas e fabricadas¹ (Gelfert, 2018). Estas notícias não são apenas fabricadas sem qualquer base na realidade, mas são frequentemente concebidas para parecerem plausíveis e manipularem o público, explorando emoções e preconceitos para maximizar o seu impacto (DSN, 2022)². São supostamente notícias criadas a partir da fantasia (uma vez que não têm qualquer relação com a realidade). Com base na Tabela 1, talvez seja mais fácil defini-las por oposição: não são notícias reais mas descontextualizadas, nem notícias exageradas (mais uma vez, reais) nem notícias inexactas (com elementos reais) (DSN, 2023a). É fundamental diferenciar *as fake news* de outros tipos de desinformação, como as notícias descontextualizadas ou exageradas, pois estas últimas, embora potencialmente enganadoras, baseiam-se em factos reais, o que as distingue das notícias completamente fabricadas (DSN, 2022). Particularmente útil é o modelo analítico de desinformação proposto por Badillo e Arteaga (2024) apresentado na Figura 1.

¹ No entanto, não é um termo pacificado (Carson, 2018) e, embora se note uma evolução no sentido da diferenciação concetual, há autores (Flores, 2022) e sobretudo no mundo jornalístico (IFJ, 2018), em que "argumentos" como o simples facto de algo ser falso invalidam que seja notícia (Mayoral, Parratt & Morata, 2019).

² A utilização da inteligência artificial amplificou esta capacidade, permitindo a criação de *deepfakes* e outros tipos de conteúdos manipulados que podem ser distribuídos em massa com grande rapidez e alcance (DSN, 2023a).

Figura 1



A pós-verdade³ é um fenómeno multifacetado (Caridad-Sebastián et al, 2018), onde a verosimilhança (Rodrigo Alsina, 2005) é mais relevante (Rodrigo Alsina, 2005), ou seja, credível, independentemente de factos verdadeiros ou reais (Dahlgren, 2018). Na pós-verdade, as emoções e as crenças pessoais prevalecem sobre os factos objetivos, o que tem implicações profundas na democracia e na coesão social, pois permite que narrativas emotivas e muitas vezes enganadoras prevaleçam no discurso público (DSN, 2022; DSN, 2024). Este fenómeno não só altera a perceção individual, como também facilita a criação de "câmaras de eco"⁴ em que as pessoas são repetidamente expostas às mesmas ideias, reforçando as suas crenças e isolando-as de outras perspectivas (DSN, 2023a).

Existem também múltiplas definições de desinformação, que sofreram mutações ao longo do tempo e dependendo do sector ou campo onde são utilizadas ou delineadas (Arteaga, 2020). Este termo engloba não só a disseminação intencional de informações falsas, mas também a manipulação subtil de factos para distorcer a realidade e confundir

³ Não existe uma posição única, mas ao contrário do conceito anterior (e matizado), existe um consenso maioritário sobre o elemento central do "querer acreditar" em detrimento dos factos ou da realidade (Olmo, 2019). O fenómeno "é mentira, mas pode ser verdade" <https://twitter.com/hematocritico/status/1241797239779069952?lang=es>

⁴ Uma *câmara de eco* é um fenómeno em que as informações, opiniões e crenças são reforçadas e amplificadas dentro de um grupo ou comunidade fechada, limitando a exposição a diferentes perspectivas (Jamieson e Cappella, 2008). Para mais informações sobre as câmaras de eco, ver: *The echo chamber is overstated* (Dubois e Blank, 2018). <https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract>

o público (DSN, 2022). A DSN, em consonância com os postulados da UE, define-a como *"A desinformação é uma informação comprovadamente falsa ou enganosa que é criada, apresentada e divulgada com fins lucrativos ou para enganar deliberadamente o público, e é suscetível de causar danos públicos"* (DSN, 2022, p.253).

Apesar de adequada, esta definição restringe ou minimiza alguns dos elementos que constam da Estratégia Nacional de Segurança⁵, como a referência ao domínio cognitivo (DSN, 2021) ou a ênfase na intencionalidade e nos objectivos de quem leva a cabo campanhas de desinformação (conferindo-lhe assim um contexto). O impacto cognitivo da desinformação é crucial, pois não se trata apenas de difundir informações falsas, mas também de alterar a percepção e o julgamento do público, corroer a confiança nas instituições e fomentar a polarização social (DSN, 2022; DSN, 2023a). Esta opinião coincide com a de outros autores como Artega e Olmo, que referem que "a desinformação permite fragmentar, isolar e manipular opiniões públicas infectadas, desacreditar e questionar factos objectivos e acreditar emoções virtuais e percepções induzidas como reais" (Artega, 2020) e "quando a falsidade se torna mais subtil, mais complexa, foi criada com intencionalidade táctica, responde a uma estratégia e persegue objectivos, é quando podemos falar de desinformação" (Olmo, 2019).

3. ESTRATÉGIAS HÍBRIDAS E ZONA CINZENTA

As estratégias híbridas são definidas como uma abordagem ao conflito que combina elementos convencionais e não convencionais, utilizando uma variedade de ferramentas - militares, económicas, diplomáticas, cibernéticas e de informação - para alcançar objetivos estratégicos (Colom, 2018). Estas ferramentas incluem não só a manipulação direta da informação, mas também a criação de narrativas que alteram a percepção pública a longo prazo, uma característica central tanto das operações de influência como da desinformação (Torres Soriano, 2022). A utilização destas estratégias justifica-se pela sua capacidade de explorar vulnerabilidades através de uma abordagem que integra o militar com outros domínios, como o cognitivo e o informacional, criando uma sinergia que multiplica a sua eficácia em contextos de baixa intensidade (Walker, 1998).

A zona cinzenta, por sua vez, caracteriza-se pela aplicação de táticas destinadas a permanecer abaixo do limiar que desencadearia uma guerra aberta. Este conceito é fundamental para compreender como os actores estatais e não estatais desafiam a ordem internacional sem ultrapassar as linhas vermelhas que conduziriam a um conflito armado (Martín Renedo, 2022). Na prática, as operações na zona cinzenta vão desde a coerção económica e a utilização da desinformação até ao emprego de forças especiais em missões secretas, concebidas para serem difíceis de atribuir diretamente a um Estado (McCuen 2008). A sobreposição entre os planos físico, virtual e cognitivo na zona cinzenta permite que estas estratégias sejam executadas de forma mais eficaz, uma vez que a percepção do conflito é manipulada para desorientar as populações-alvo e enfraquecer a sua capacidade de resposta (Lupiáñez Lupiáñez, 2023).

⁵ Embora esta definição seja precisa, é importante considerar que a desinformação também pode ser motivada por objectivos não políticos ou não ideológicos, como o crime organizado ou a procura de lucro por parte de actores não estatais (DSN, 2023a; Marchal González, 2023).

Estratégias híbridas⁶ e a "zona cinzenta" são uma evolução das táticas e estratégias históricas da guerra irregular, agora reforçadas pela tecnologia moderna e pelas redes de informação, permitindo uma influência mais eficaz e menos detetável num contexto global (Hafen, 2024). A desinformação, a propaganda e as operações de influência são componentes essenciais destas estratégias, que são utilizadas num ambiente cada vez mais complexo e globalizado (Hoffman, 2009).

A propaganda moderna vai além da simples disseminação de mensagens; é uma manipulação sofisticada da informação para moldar percepções e comportamentos de acordo com os interesses estratégicos daqueles que a promovem (Calvo Albero, 2017). A propaganda⁷ pode ser vista como uma extensão das operações psicológicas, em que o objetivo não é apenas influenciar a opinião pública, mas também desmoralizar o adversário e alterar a sua capacidade de decisão (Rid, 2021)⁸. Desde 2023, estas operações têm-se intensificado, sobretudo no contexto de conflitos globais como os da Ucrânia e de Gaza, onde a propaganda tem desempenhado um papel crucial na polarização da opinião pública e na manipulação da informação à escala internacional (DSN, 2024).

Neste contexto, a desinformação não só actua como uma ferramenta de influência, mas também facilita outras operações híbridas ao enfraquecer a coesão social e a confiança nas instituições, criando um ambiente propício à implementação de táticas mais agressivas sem a necessidade de um confronto militar aberto (Alastuey Rivas et al., 2024). É crucial compreender que as estratégias híbridas não são um fenómeno novo, mas sim uma evolução das táticas de guerra irregular que têm sido empregues ao longo da história, embora as mudanças sociais e o avanço da tecnologia tenham expandido muito as ferramentas disponíveis para estas estratégias, permitindo a sua aplicação à escala global e com um impacto significativo na estabilidade internacional (Calvo, 2023). Este facto pode ser claramente observado na Doutrina Primakov/Gerasimov russa, na conceção chinesa das "Três Guerras" ou na "Nova Conceptualização da Zona Cinzenta" ocidental (Adame Hernández, 2024).

3.1. MANIPULAÇÃO E INTERFERÊNCIA DE INFORMAÇÕES ESTRANGEIRAS (FIMI)

O conceito de *Manipulação e Interferência de Informação Estrangeira* (FIMI) refere-se a actividades deliberadas levadas a cabo por actores estrangeiros com o objetivo de distorcer informação, manipular a perceção pública e influenciar processos políticos e sociais noutros países. De acordo com o relatório conjunto da Agência da União Europeia para a Cibersegurança (ENISA) e do Serviço Europeu para a Ação Externa (SEAE), a FIMI engloba uma variedade de acções, incluindo a disseminação de desinformação, propaganda e operações psicológicas que procuram semear a discórdia e desestabilizar as sociedades democráticas (ENISA & SEAE, 2022). A FIMI pode também envolver a

⁶ Embora o conceito de "guerra híbrida" tenha sido objeto de múltiplas definições e debates, continua a não haver consenso sobre a sua caracterização precisa, o que complica o seu estudo e aplicação na análise estratégica contemporânea (Colom, 2018b).

⁷ Especificamente, a propaganda é definida como um "conjunto de técnicas utilizadas, de forma sistemática, para difundir opiniões ou ideias parciais ou tendenciosas entre as massas, com uma intenção própria, muitas vezes política" (Donoso Rodríguez, 2020, p. 30), o que a torna uma ferramenta fundamental nas operações psicológicas.

manipulação de narrativas culturais e históricas para alimentar conflitos internos e desestabilizar a ordem social, explorando questões sensíveis que ressoam com preconceitos ou receios existentes numa sociedade (Buvarp, 2021). A sofisticação destas operações reside na sua capacidade de explorar clivagens pré-existentes nas sociedades-alvo, exacerbando divisões e provocando reacções que minam a coesão social e política (Allenby e Garreau, 2017). Estas actividades podem ter consequências profundas para a estabilidade das instituições democráticas, uma vez que se centram na exploração de vulnerabilidades sociais e políticas (ENISA & SEAE, 2022).

No contexto das FIMI, é essencial reconhecer que estas operações nem sempre envolvem a disseminação de informações completamente falsas. Muitas vezes, assentam em distorções subtis de factos reais, recorrendo a técnicas como a saturação de informação ou a criação de bolhas de informação (Rid, 2021); dificultando a deteção e a resposta. Estas estratégias, designadas por "manipulação subtil da verdade", são particularmente perigosas porque jogam com a perceção pública e a credibilidade das fontes de informação (Castro Torres, 2021). Além disso, a manipulação da informação através de canais não tradicionais, como as redes sociais e as plataformas de mensagens instantâneas, permite que os actores estrangeiros maximizem o impacto das suas campanhas, tirando partido das características virais e do alcance global destas ferramentas (EEAS, 2024).

A FIMI está enquadrada em estratégias híbridas. A propaganda e as acções de influência são instrumentos fundamentais no quadro da FIMI. A propaganda é utilizada para promover narrativas que favorecem os interesses do ator estrangeiro, recorrendo a meios de comunicação controlados ou equiparados para divulgar mensagens específicas. Estas narrativas são cuidadosamente concebidas para parecerem legítimas e recorrem muitas vezes a fontes tendenciosas ou tendenciosas que conferem credibilidade às mensagens divulgadas (Maggioni e Magri 2015). Narrativas concebidas para gerar desconfiança em relação às instituições democráticas e polarizar a sociedade (Bennett & Livingston, 2020). Além disso, as acções de influência visam moldar a opinião pública ou influenciar as decisões políticas, o que pode incluir desde a manipulação das redes sociais até ao financiamento encoberto de actores políticos ou mediáticos no país alvo (EEAS, 2023). Um exemplo recente desta situação foi observado nas eleições presidenciais romenas (Comissão Europeia, 2024). O anonimato proporcionado pelas plataformas digitais e a possibilidade de operar através de intermediários ou *proxies* acrescenta uma camada de complexidade ao rastreio e à identificação dos verdadeiros autores destas campanhas, dificultando a aplicação de contramedidas eficazes (Castro Torres, 2021). A utilização destes métodos permitiu que os intervenientes estrangeiros operassem com uma camada adicional de anonimato e negação, complicando os esforços para identificar e combater estas actividades (DSN, 2024).

4. DOMÍNIO COGNITIVO E DESINFORMAÇÃO

Embora a concetualização do domínio cognitivo seja relativamente moderna, as estratégias para operar nele, como a propaganda (Calvo, 2023), a influência (Jordán, 2018) e a desestabilização (Quiñones de la Iglesia, 2021) não o são. Estas tácticas têm sido historicamente utilizadas em diversos contextos geopolíticos, evoluindo ao longo do tempo para se adaptarem às novas tecnologias da informação e às dinâmicas sociais em mudança. Por exemplo, a propaganda, que outrora dependia exclusivamente dos meios de comunicação tradicionais, como a imprensa escrita e a rádio, está agora dispersa por

plataformas digitais e redes sociais, permitindo uma maior penetração e rapidez na disseminação das mensagens. Estas ferramentas adquiriram uma sofisticação sem precedentes, tirando partido da velocidade e do alcance da Internet e das redes sociais para amplificar os seus efeitos, como se verifica nas tácticas utilizadas por grupos como a Al-Qaeda e o Estado Islâmico, que têm utilizado estas tecnologias para influenciar a opinião pública mundial e legitimar as suas acções (Astorga González, 2020). A influência das plataformas digitais é tal que permite a actores maliciosos segmentar audiências e personalizar mensagens, criando câmaras de eco que reforçam crenças pré-existentes e impedem a disseminação de informação contrária. Esta situação é potenciada pela utilização de algoritmos que favorecem a polarização ao dar prioridade a conteúdos sensacionalistas e de carga emocional, o que, por sua vez, facilita a manipulação do domínio cognitivo em grande escala (DSN, 2023b).

A teoria estruturalista da construção ideológica de Louis Althusser, em que os meios de comunicação social desempenham um papel central na criação e manutenção de ideologias que dominam a perceção pública, reforça a compreensão de como as tácticas de desinformação estão inseridas no domínio cognitivo⁹ (Althusser, 1971). Em consonância com isto, a manipulação do domínio cognitivo envolve a criação de realidades percebidas que, embora não reflectam necessariamente a realidade objetiva, se tornam a base sobre a qual são tomadas decisões políticas e sociais (Lupiáñez Lupiáñez, 2023). Como referem vários autores, como Foucault, a linguagem não só descreve o mundo, mas também actua sobre ele (Foucault, 1972), o que reforça a ideia de que o domínio cognitivo pode ser manipulado através da construção de narrativas que reconfiguram a realidade percebida.

Em relação à desinformação, a zona cinzenta centrar-se-á principalmente em estabelecer o contexto, utilizando estratégias como a propaganda ou a desinformação, com o objetivo de obter gradualmente uma vantagem estratégica sobre o adversário, o que facilitaria a melhoria da eficácia de futuras intervenções (Hernández-García, 2022). Libicki reforça esta ideia explicando como as operações cognitivas nem sempre procuram resultados imediatos, mas podem ser concebidas para semear a dúvida e a confusão, afectando a capacidade do adversário para tomar decisões eficazes a longo prazo (Libicki, 2021). Esta abordagem sublinha a importância do gradualismo na estratégia de desinformação, onde pequenas mudanças na perceção e na narrativa podem culminar numa alteração significativa da realidade percebida, fazendo com que o adversário perca a iniciativa e o controlo sobre a situação. Nesta abordagem, deve ser realçada a concordância entre objectivos, visão estratégica e gradualismo.

A relação entre a manipulação cognitiva e o conflito político também pode ser analisada numa perspectiva Clausewitziana. Clausewitz defende que a guerra é um ato político racional em que se procura desmoralizar o adversário não só através do conflito direto, mas também através da manipulação das paixões da população e da perceção da realidade (Clausewitz, 1976). Através da desinformação é possível corroer a moral de um exército inimigo e, mais significativamente ainda, da sua população, com o objetivo de

⁹ A doutrina militar espanhola sublinha a relevância do STRATCOM (*Comunicações Estratégicas*) como uma função de gestão que integra as INFOOPS (*Operações de Informação*) e as PSYOPS (*Operações Psicológicas*), aplicando técnicas de engenharia social e de comunicação estratégica para moldar o ambiente informacional e cognitivo. Estas capacidades permitem às Forças Armadas atingir objectivos que transcendem os meios convencionais, operando num domínio intangível que permeia todos os outros domínios (PDC-01, 2018).

persuadir os seus decisores políticos a cessar a sua atitude beligerante, a levar a cabo uma negociação ou a obter benefícios numa negociação já planeada (Rodríguez Lorenzo et al, 2023).

Um fator fundamental a ter em conta, e que muitas vezes só é abordado de forma colateral, é a relação e o impacto políticos. Este aspeto, embora crucial, é muitas vezes subestimado nas análises da desinformação, onde é dada maior ênfase aos aspectos técnicos ou táticos, deixando de lado as implicações mais amplas para a governação e a estabilidade política. Numa lógica clausewitziana, "se a guerra é política por natureza, é evidente que o alvo principal não são as forças armadas do inimigo, mas a liderança política" (Calvo Albero, 2017).

É a intersecção entre a desinformação utilizada em estratégias híbridas e de zona cinzenta; com os objectivos perseguidos (sobretudo a afetação política) onde se ligam à sociedade, à agenda e à opinião pública (Sartori, 2007). Neste contexto, a manipulação da informação e a criação de narrativas alternativas não têm apenas impacto a nível estatal ou militar, mas têm também profundas implicações no tecido social e cultural. A construção destas narrativas, que utilizam o cinema e os media¹⁰ como ferramentas de manipulação emocional, continua a ser central para compreender como as narrativas maliciosas podem dividir e confundir a sociedade (Davis, 2005). A capacidade destas estratégias para alterar a perceção pública não se deve apenas à sofisticação das táticas empregues, mas também à forma como estas narrativas se alinham com preocupações e medos existentes na sociedade, amplificando-os e redireccionando-os contra alvos específicos (Castro Torres, 2021).

A construção de narrativas maliciosas, que procuram dividir e confundir a sociedade, torna-se uma ferramenta poderosa para desestabilizar não só os governos, mas também as comunidades e a coesão social no seu conjunto. A necessidade de criar uma narrativa maliciosa que possa ser explorada em proveito próprio (Rodríguez Lorenzo et al, 2023), uma narrativa atractiva que sustente a estratégia híbrida (Torres, 2022) e a geração inelutável de uma narrativa que patrocine, cubra, reforce e proteja a zona cinzenta (Hernández-García, 2022), conferem um grande papel aos quadros cognitivos (Goffman, 2006), à comunicação persuasiva (Candelas, 2023) e à opinião pública (Sartori 2007). Estes elementos, embora subestimados em muitas análises, são fundamentais para compreender como a desinformação se insere no tecido social e se torna uma força de mudança, corroendo a confiança nas instituições e alterando a perceção da realidade. Compreender a relação entre manipulação cognitiva e mudança social é crucial porque, tal como descrito por Berger e Luckmann (2003), a construção social da realidade é um processo dinâmico (externalização, objectivação e internalização) que pode ser facilmente influenciado por actores com controlo sobre os media (interacção social) e as narrativas (linguagem).

¹⁰ Um exemplo muito eloquente é a utilização da comunicação mais tradicional (como o cinema) e da comunicação digital (vídeos de alta qualidade e elevada qualidade de produção divulgados *online*) nas estratégias de comunicação de organizações tão pouco "ocidentais" como o *Daesh*. Com o recurso, para além dos aspectos técnicos, a táticas emocionais e à exploração de enviesamentos cognitivos como a ancoragem, tornaram-se componentes fundamentais para moldar a perceção do conflito (Astorga González, 2020).

5. CONSTRUIR NARRATIVAS E ENQUADRAMENTOS

As narrativas são narrativas estruturadas que procuram dar sentido aos acontecimentos e moldar a percepção do público. Desde a antiguidade, a propaganda tem-se baseado na construção de narrativas que moldam a percepção pública. Foi descrito como são criadas "ilusões necessárias"¹¹ para que certos grupos de poder mantenham a sua influência sobre a sociedade (Herman & Chomsky, 1988). No contexto da desinformação moderna, as narrativas são concebidas não só para convencer, mas também para enraizar crenças que são difíceis de erradicar, mesmo quando expostas como falsas¹². Flynn, Nyhan e Reifler (2017) identificam que as percepções políticas erróneas não são simples falhas de informação, mas devem-se a percepções erróneas (crenças falsas ou infundadas mantidas com confiança e resistência à correção), factores individuais (como preconceitos cognitivos ou identidades partidárias ou ideológicas) e resistência à mudança (passiva à apuração de informações falsas ou processos de verificação de factos); mas também ambientes mediáticos e políticos (facilitando a exposição selectiva às fontes).

Essas narrativas, uma vez implantadas, podem continuar a exercer um efeito duradouro devido à inércia cognitiva e à resistência à mudança de crenças estabelecidas (Libicki, 2021; Flynn, Nyhan, & Reifler, 2017). As narrativas falsas e altamente enganosas tendem a prevalecer devido à sua capacidade de explorar as emoções humanas, como o medo e a indignação moral, o que aumenta o seu impacto e disseminação nas redes sociais (Pennycook & Rand, 2021).

O conceito de *enquadramento* refere-se às estruturas cognitivas que determinam a forma como interpretamos e compreendemos a informação. Estes enquadramentos actuam como atalhos mentais que organizam a informação e nos permitem interpretar os acontecimentos de acordo com esquemas prévios de significado. A teoria dos enquadramentos cognitivos destaca a forma como as estruturas interpretativas que a sociedade utiliza para dar sentido aos acontecimentos podem ser manipuladas através da comunicação persuasiva (Goffman, 2006). A disputa pelo controlo destes enquadramentos tornou-se um elemento central na luta contra a desinformação; o *enquadramento* não só procura combater as falsidades, mas também estabelecer enquadramentos alternativos que reconfigurem o debate público (Tuñón Navarro, Oleart, & Bouza García, 2019). No contexto das estratégias híbridas e, por extensão, do domínio cognitivo, os enquadramentos são utilizados para focar a atenção pública em determinados aspetos da realidade, ao mesmo tempo que ocultam ou distorcem outros¹³. Este processo permite que determinadas narrativas prevaleçam, não pela sua veracidade, mas pela forma como são apresentadas e contextualizadas. Este processo é fundamental

¹¹ Em *Manufacturing Consent: The Political Economy of the Mass Media* (Herman & Chomsky, 1988), a expressão "ilusões necessárias" não é encontrada como citação textual. No entanto, o conceito é desenvolvido ao longo do livro. O conceito de "ilusões necessárias" vem da obra posterior *Necessary Illusions* (Chomsky, 1992).

¹² De acordo com investigações recentes, a suscetibilidade à desinformação não é apenas motivada pelo partidarismo, mas também pela falta de raciocínio cuidadoso e pela utilização de heurísticas, como a familiaridade com a informação e a credibilidade da fonte (Pennycook et al, 2021).

¹³ A investigação sugere que a interação entre as redes sociais e a psicologia humana, em particular a tendência para utilizar atalhos mentais e confiar na familiaridade, contribui significativamente para a difusão e persistência de notícias falsas (Pennycook et al, 2021).

para manter o controlo narrativo e impedir que as premissas fundamentais das acções empreendidas num conflito sejam questionadas (Colom, 2018).

Na prática moderna, o *enquadramento* tornou-se uma ferramenta fundamental não só para moldar a interpretação dos acontecimentos, mas também para influenciar as emoções da audiência, explorando preconceitos cognitivos que dificultam a reflexão crítica (Astorga González, 2020).

5.1. APLICAÇÃO

A construção de narrativas e enquadramentos no contexto da desinformação envolve um processo complexo de criação de narrativas e estruturas cognitivas destinadas a influenciar a percepção pública de forma profunda e duradoura. Este processo baseia-se numa compreensão avançada da ciência comportamental, em que os enviesamentos cognitivos como a ancoragem, a disponibilidade e a confirmação são explorados para garantir que as narrativas construídas são resistentes à mudança (Astorga González, 2020). A sofisticação na construção destas narrativas emprega a capacidade de combinar factos reais com distorções subtis, tornando-os mais difíceis de desacreditar e mais fáceis de aceitar pela audiência (Rid, 2021). Desta forma, as narrativas, que exploram os vieses cognitivos e emocionais da audiência, são estruturadas para serem simplificadas e emocionais, o que aumenta a sua eficácia na manipulação dos media (Herman & Chomsky, 1988). Estas narrativas procuram não só convencer, mas também estabelecer uma percepção da realidade que é resistente à correção, mesmo quando a sua falsidade é exposta¹⁴. A exposição repetida a notícias falsas aumenta a sua credibilidade percebida, mesmo quando inicialmente são plausíveis. Este efeito, conhecido como a "ilusão da verdade", desempenha um papel crucial na permanência e aceitação de narrativas falsas (Pennycook et al, 2021).

Além disso, o *microtargeting* ou segmentação da população de acordo com as suas crenças e valores permitiu que as mensagens fossem adaptadas especificamente a cada grupo, o que, juntamente com a proliferação de meios e canais alternativos (e por vezes opacos para a maioria da população e da opinião pública), amplificou a capacidade destes quadros para influenciar a percepção pública, aumentando a eficácia da manipulação (Astorga González, 2020). Esta abordagem personalizada da disseminação da desinformação maximiza o impacto em diferentes segmentos da sociedade, fomentando a polarização e reforçando crenças pré-existentes, ao mesmo tempo que dificulta a deteção (Maggioni e Magri, 2015).

O impacto destas narrativas e enquadramentos é tal que, mesmo quando desacreditados, podem continuar a influenciar a opinião pública devido à inércia cognitiva, um fenómeno em que as crenças previamente estabelecidas são resistentes à mudança (Libicki, 2021). Isto é particularmente evidente na forma como certos quadros narrativos persistem no discurso público muito depois de terem sido provados falsos, continuando a influenciar a percepção e a ação social (Juurvee e Mattiisen, 2020). Desta

¹⁴ Outro exemplo seria a "guerra memética", que utiliza memes e outras formas de desinformação viral, procura criar e disseminar narrativas que alteram as percepções e as emoções do público-alvo, alcançando um impacto duradouro que é difícil de contrariar, especialmente quando envolve conteúdo de paródia e fontes civis (Arias Gil, 2019).

forma, a construção de narrativas e enquadramentos torna-se uma ferramenta poderosa para moldar a percepção pública e manter o controlo sobre a interpretação da realidade.

5.2. IMPACTO DAS NARRATIVAS E DOS QUADROS NO DOMÍNIO COGNITIVO

As narrativas e os enquadramentos têm um impacto profundo no domínio cognitivo, moldando não só a forma como os acontecimentos são percebidos, mas também a forma como são compreendidos e recordados. Foi observado que a criação de uma narrativa maliciosa pode ser explorada em benefício daqueles que controlam a narrativa, dando grande poder aos quadros cognitivos e à comunicação persuasiva (Rodríguez Lorenzo et al, 2023; Torres, 2022). Esses elementos são fundamentais para entender como a desinformação se incorpora ao tecido social e se torna uma força de mudança, corroendo a confiança nas instituições e alterando as percepções da realidade. Além disso, estes quadros não só influenciam a percepção individual, como também afectam a memória colectiva, condicionando a forma como as sociedades recordam e aprendem com os acontecimentos históricos, o que pode ter repercussões a longo prazo na coesão social e na formação das identidades nacionais (Aznar Fernández-Montesinos, 2021). A propaganda e a desinformação não operam apenas através de mensagens diretas, mas também moldam o ambiente cognitivo em que essas mensagens são interpretadas, criando um ambiente de incerteza e desconfiança que facilita a manipulação da opinião pública (Lupiáñez Lupiáñez, 2023).

A manipulação cognitiva provou ser capaz de alterar não só a percepção imediata da realidade, mas também de moldar padrões de pensamento e comportamento a longo prazo (Astorga González, 2020). O impacto destas narrativas no domínio cognitivo é amplificado pela utilização de tecnologias da informação que permitem uma disseminação rápida e massiva, o que torna os efeitos da desinformação mais duradouros e difíceis de contrariar (Lupiáñez Lupiáñez, 2023).

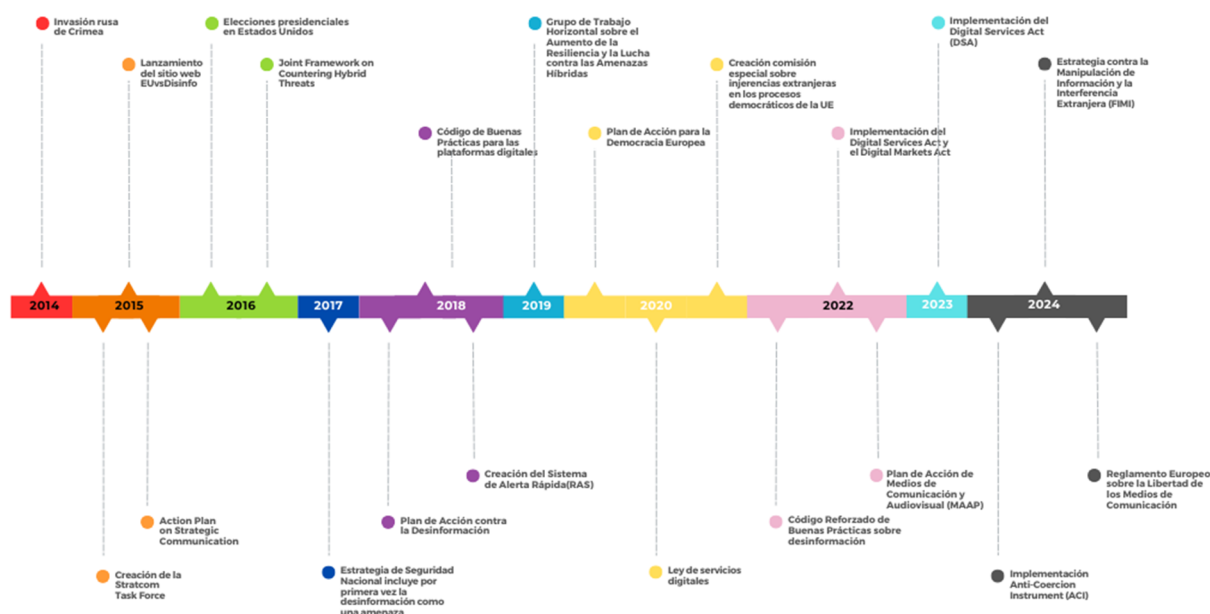
6. EVOLUÇÃO DA DESINFORMAÇÃO

A UE implementou um conjunto de políticas e acções coordenadas para combater a desinformação, reconhecendo o seu impacto significativo na estabilidade democrática e na segurança dos Estados-Membros. A relevância desta ameaça intensificou-se após acontecimentos como a invasão russa da Crimeia, em 2014, e as eleições presidenciais norte-americanas de 2016, que puseram em evidência a forma como a desinformação pode ser utilizada como um instrumento eficaz em conflitos híbridos e na interferência eleitoral (SEAE, 2015). Os principais marcos podem ser vistos na Figura 2 .¹⁵

¹⁵ Para mais informações sobre a evolução das acções da UE, ver *Espanha face à desinformação: Desafios híbridos e respostas convencionais* (Adame Hernández, 2024).

Figura 2

LAS POLÍTICAS DE LA UNIÓN EUROPEA EN LA LUCHA CONTRA LA DESINFORMACIÓN



Fonte: Elaboração própria.

Em Espanha, a perceção da desinformação evoluiu significativamente nas últimas décadas, a partir da segunda metade da década de 2010, marcada por um crescente reconhecimento dos riscos associados à circulação de informações falsas e manipuladas, tanto a nível nacional como internacional (Badillo e Arteaga, 2024).

A polarização política em Espanha, acentuada pelo conflito na Catalunha e pela crescente fragmentação do espectro político, tem sido um fator relevante na perceção da desinformação (Badillo e Arteaga, 2024). Sessenta por cento dos espanhóis consideram que existe uma grande divisão política no país e mais de 70 por cento consideram que a desinformação está a contribuir significativamente para essa divisão (CIS, 2021).

A confiança dos espanhóis nos meios de comunicação social continua a ser baixa (inferior a 5 em 10)¹⁶, enquanto a influência das redes sociais está a aumentar¹⁷ (CIS, 2024). O índice de confiança nos meios de comunicação social, elaborado pelo Eurobarómetro, revela uma significativa falta de confiança entre os espanhóis. Quarenta por cento dos inquiridos em Espanha não confiam nos meios de comunicação tradicionais, 12 pontos acima da média europeia, e 58% acreditam que os meios de comunicação fornecem informações sujeitas a pressões políticas ou comerciais, 15 pontos acima da média europeia (Eurobarómetro, 2024).

¹⁶ Numa escala de 1 a 10 sobre a confiança que têm nos meios de comunicação social, a confiança passou de 4,3 em 2021 para 4,2 em 2022 e 4,1 em 2023 e 2024. A tendência é mais acentuada à medida que diminui com a idade: o grupo etário 25-34 classifica-a em 2,88 e o grupo etário 18-24 em 3,45 (CIS, 2024).

¹⁷ A percentagem de espanhóis influenciados pelas redes sociais e pela Internet na tomada de decisões políticas aumentou de 8,6 % em 2021 para 9,4 % em 2022, 10,3 % em 2023 e 16,2 % em 2024 (CIS, 2024).

A digitalização e a penetração das redes sociais desempenharam um papel crucial na evolução da percepção da desinformação. De acordo com o Índice de Economia e Sociedade Digital (DESI) 2024, a Espanha registou um aumento constante na utilização da Internet e das redes sociais. O DESI indica que, em 2024, 96,45% dos agregados familiares espanhóis tinham acesso à Internet, 88,23% da população possui competências digitais superiores¹⁸ e 34,4% das empresas utilizam várias redes sociais (em comparação com 28,5% da média europeia (DESI, 2020)). Este elevado nível de conectividade aumentou a exposição da população a campanhas de desinformação. A importância crescente das redes sociais como principal canal de acesso à informação¹⁹, especialmente entre os jovens²⁰, sugere um afastamento dos formatos tradicionais de notícias e uma preferência por conteúdos visuais e breves (Reuters Institute for the Study of Journalism, 2024).

Por último, o contexto global também influenciou a percepção da desinformação em Espanha. A pandemia de COVID-19, por exemplo, desencadeou uma "infodemia", um termo cunhado pela Organização Mundial de Saúde para descrever a superabundância de informações, tanto precisas como imprecisas, que tornou difícil para as pessoas encontrarem fontes confiáveis (OMS, 2020). Durante a pandemia, a rede Latam Chequea verificou mais de 1.000 notícias falsas relacionadas com a COVID-19 em Espanha, muitas das quais foram amplamente difundidas nas redes sociais e nas aplicações de mensagens (Latam Chequea, 2022). Este fenómeno exacerbou a desconfiança do público e desestabilizou ainda mais o ecossistema de informação, sublinhando a necessidade de reforçar as capacidades nacionais para detetar e combater eficazmente a desinformação (OCDE (2024)). Num contexto de desconfiança crescente em relação aos meios de comunicação social tradicionais, que afecta quase 70% da população (Novoa-Jaso, Sierra, Labiano, & Vara-Miguel, 2024). Além disso, 37% dos espanhóis evitam ativamente as notícias, um comportamento que parece ser motivado pela saturação de conteúdos negativos ou controversos que dominam as narrativas actuais dos meios de comunicação social (Reuters Institute for the Study of Journalism, 2024).

A resposta institucional da Espanha à desinformação evoluiu significativamente desde 2017, quando o problema foi reconhecido pela primeira vez na Estratégia Nacional de Segurança, até a implementação de políticas mais robustas e coordenadas nos anos seguintes. No entanto, esta evolução tem sido marcada tanto por avanços notáveis como por algumas deficiências na integração de abordagens mais holísticas que incluem a gestão de narrativas (Adame Hernández, 2024).²¹

¹⁸ Estas incluem o envio/receção de correio eletrónico; chamadas telefónicas ou de vídeo através da Internet; mensagens instantâneas; participação em redes sociais; expressão de opiniões sobre questões cívicas ou políticas em sítios Web ou redes sociais; participação em consultas ou votações em linha sobre questões cívicas ou políticas.

¹⁹ O WhatsApp ultrapassou o Facebook como a principal fonte de informação em Espanha, com 36% dos utilizadores a utilizarem o WhatsApp para aceder a notícias, em comparação com 29% que utilizam o Facebook. Esta transição evidencia uma mudança para plataformas mais privadas e centradas no envio de mensagens (Reuters Institute for the Study of Journalism, 2024).

²⁰ O TikTok e o Instagram estão a crescer rapidamente entre os menores de 25 anos. O TikTok é utilizado por 30% deste grupo etário para obter informações, enquanto o Instagram atinge 25%, ultrapassando plataformas mais tradicionais como o YouTube, que se situa nos 15% (Reuters Institute for the Study of Journalism, 2024).

²¹ Para mais informações sobre a evolução das políticas de Espanha contra a desinformação, ver *España frente a la desinformación: Desafíos híbridos y respuestas convencionales* (Adame Hernández, 2024).

7. MEDIDAS E INSTRUMENTOS ACTUAIS DE COMBATE À DESINFORMAÇÃO EM ESPANHA

O núcleo da infraestrutura espanhola de combate à desinformação centra-se na Comissão Permanente contra a Desinformação, que coordena a resposta operacional às campanhas de desinformação. Esta comissão actua sob a supervisão da Secretaria de Estado da Comunicação, que lidera a política de comunicação estratégica do governo. Em situações de crise, a Célula de Coordenação da Desinformação gere a resposta, assegurando que as acções do Governo são rápidas e eficazes (ORDEN PCM/1030/2020, 2020).

O Fórum contra as Campanhas de Desinformação na Esfera da Segurança Nacional tem sido um dos principais pilares da estratégia espanhola contra a desinformação. Em 2023, foram apresentados sete trabalhos que abordam várias facetas do problema, desde metodologias de verificação e prevenção (como o *prebunking* e a teoria da inoculação²²) até à análise da desinformação russa no contexto da guerra na Ucrânia (DSN, 2023b). No final de 2024, apresentaram a segunda edição dos trabalhos do Fórum, avançando em aspectos como o papel dos media e dos departamentos de comunicação de instituições públicas e privadas, o FIMI, a ligação entre desinformação e discurso de ódio, e hipóteses de trabalho sobre o ecossistema mediático espanhol e a opinião pública em relação à desinformação (DSN, 2024b). O Fórum canaliza a cooperação público-privada e público-social, articulando uma abordagem estratégica e multisectorial. A profundidade das suas análises, bem como os seus esforços para abordar uma realidade complexa, são claramente evidenciados na evolução das suas respectivas publicações.

Ou outras iniciativas como as campanhas de comunicação positiva do Ministério dos Negócios Estrangeiros, da União Europeia e da Cooperação para combater a desinformação através de narrativas verificáveis²³, o desenvolvimento de ferramentas tecnológicas como o ELISA²⁴ (Estudo Simplificado de Fontes Abertas) ou o projeto DANGER (INCIBE, (2024), o Plano de Ação para a Democracia²⁵ (MPJRC, 2024) ou o despacho que estabelece a elaboração da Estratégia Nacional contra as Campanhas de Desinformação (Despacho PJC/248/2025, 2025). É de salientar a ausência de estudos, relatórios ou análises sobre o impacto das medidas institucionais contra a desinformação.

7.1. PROCEDIMENTO DE ACÇÃO CONTRA A DESINFORMAÇÃO

O Procedimento de ação contra a desinformação regulado pela Ordem PCM/1030/2020, tem como objetivo fundamental a criação de um quadro coordenado para detetar, analisar

²² O *prebunking* é uma técnica de comunicação preventiva que consiste em expor as pessoas a uma versão enfraquecida da desinformação antes de a encontrarem, a fim de aumentar a sua resistência e capacidade crítica contra futuras tentativas de manipulação. Esta estratégia é semelhante à "inoculação" psicológica, que procura gerar imunidade cognitiva contra narrativas falsas (Maldita.es, 2023; Roozenbeek et al., 2022).

²³ Destaque para as campanhas "Voto exterior", "Tu Consulado", "Viaja Seguro" e informações sobre a Ley de Memoria Democrática (DSN, 2024, p. 103).

²⁴ A ELISA monitoriza sítios Web suspeitos de promoverem campanhas de desinformação, permitindo a deteção precoce e uma resposta mais ágil por parte das autoridades (CCN-CERT, 2019). Em 2023, aumentou as suas capacidades, integrando algoritmos de inteligência artificial que lhe permitem identificar padrões de desinformação com maior exatidão (DSN, 2024).

²⁵ Que prevê, nomeadamente, a aplicação do Regulamento (UE) 2024/1083 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que estabelece um quadro comum para os serviços de comunicação social no mercado interno e que altera a Diretiva 2010/13/UE (Regulamento Europeu sobre a Liberdade dos Meios de Comunicação Social).

e responder à desinformação em Espanha (ORDEM PCM/1030/2020, 2020), particularmente em situações que afectam a segurança nacional. Este procedimento foi aprovado pelo Conselho de Segurança Nacional e insere-se no contexto das estratégias europeias de combate à desinformação, nomeadamente as estabelecidas no Plano de Ação para a Desinformação da UE de 2018.

O procedimento articula-se em quatro eixos fundamentais: deteção, análise, resposta e avaliação; e em quatro níveis de ativação. A Secretaria de Estado da Comunicação é responsável pela coordenação geral, actuando em estreita colaboração com outros ministérios, com o Centro de Situação do Conselho de Segurança Nacional e com o Grupo de Trabalho contra a Desinformação. Este grupo interministerial é responsável por aconselhar e propor acções ao Conselho de Segurança Nacional, assegurando uma resposta integrada e coerente.²⁶

A implementação do procedimento provocou controvérsia pública e levou várias organizações a apresentar recursos e queixas junto do Tribunal Contencioso-Administrativo²⁷. Também foi criticado pela falta de clareza na definição das competências e dos campos de ação das diferentes autoridades envolvidas (Gómez, 2020; Garrós Font & Santos Silva, 2021) ou pela falta de recursos especializados (Badillo & Arteaga, 2024).

O Supremo Tribunal estabeleceu limites muito claros ao trabalho e ao âmbito do "Procedimento de Ação contra a Desinformação" e dos órgãos que cria, declarando que não cria nem atribui novas competências e não pode afetar os direitos fundamentais (Supremo Tribunal, 2021). Assim, o protocolo limita-se a um plano de ação interno que se limita a estabelecer critérios de coordenação. Estabelece também uma definição legal de desinformação²⁸, algo que o procedimento não faz.

²⁶ O Anexo II estabelece o funcionamento e o modo de ação da Comissão Permanente contra a Desinformação (ORDEM PCM/1030/2020, 2020).

²⁷ Para mais informações sobre o Procedimento de Ação de Desinformação, ver *Spain in the Face of Disinformation: Hybrid Challenges and Conventional Responses* (Adame Hernández, 2024).

²⁸ De acordo com o acórdão, a desinformação é entendida como "informação verificavelmente falsa ou enganosa que é criada, apresentada e divulgada com fins lucrativos ou para enganar deliberadamente o público, e que é suscetível de causar danos públicos" (Supremo Tribunal, 2021). Esta definição é retirada do Procedimento de Ação contra a Desinformação (ORDEM PCM/1030/2020, 2020) que, por sua vez, é retirada da Comunicação da Comissão Europeia COM (2018). O Procedimento de Ação de Desinformação limitou-se, no seu ponto 1. Contexto, a reproduzir a definição da Comissão Europeia.

8. CONCLUSÕES

Ao longo do artigo, analisámos a forma como a desinformação está inserida num contexto mais vasto de táticas e estratégias geopolíticas, destacando o seu papel na FIMI. Este contexto mais amplo é enriquecido pela consideração de como os quadros narrativos são estrategicamente utilizados para orientar o debate público para narrativas específicas que favorecem os interesses daqueles que as constroem, minimizando ou distorcendo aspectos da realidade que possam contradizer esses interesses (Tuñón Navarro, Oleart, & Bouza García, 2019; Astorga González, 2020). Tem sido argumentado que a desinformação não actua como uma ferramenta isolada, mas faz parte de um conjunto coordenado de acções destinadas a influenciar a perceção pública, manipular a narrativa e criar incerteza nos processos políticos e sociais (Hoffman, 2009; McCuen, 2008).

A desinformação teve um impacto crítico em acontecimentos importantes durante a última década, afectando tanto a estabilidade institucional como a coesão social. As análises revelaram que as políticas públicas em Espanha, apesar de tentarem responder a estas ameaças, têm sido insuficientes devido à sua natureza fragmentada e predominantemente reactiva (Badillo e Arteaga, 2024). Este facto colocou as instituições espanholas numa posição vulnerável face a campanhas de desinformação cada vez mais sofisticadas, que exploraram as fragilidades da coordenação interinstitucional e a falta de uma abordagem preventiva abrangente (Bennett & Livingston, 2020).

A resposta institucional à desinformação tem sido limitada pela falta de integração entre a cibersegurança e a defesa cognitiva. O anonimato proporcionado pelas plataformas digitais e a possibilidade de operar através de intermediários ou "proxies" acrescenta uma camada de complexidade que dificulta a identificação dos verdadeiros autores destas campanhas (Castro Torres, 2021), o que fomenta a necessidade de uma estratégia mais proactiva e orientada para o futuro (Arias Gil, 2019). Embora tenham sido envidados esforços significativos para melhorar a monitorização e a resposta à desinformação, estes têm sido fragmentados e carecem da coerência necessária para enfrentar eficazmente as ameaças. Um exemplo é a ausência de uma proposta de Estratégia Nacional de Combate às Campanhas de Desinformação desde 2022 (DSN, 2022). Esta situação é claramente exemplificada pela ativação do nível 1 do Procedimento de Ação contra a Desinformação. O nível mais baixo de ativação do Procedimento envolve a concordância de organismos estatais de alto nível, como o Secretário de Estado da Comunicação, a DSN, a CNI e o Secretário de Estado da Transformação Digital e Inteligência Artificial, entre outros (ORDEN PCM/1030/2020, 2020). Atribui ainda um papel predominantemente reativo, o que reforça a limitada resposta e alcance institucional.

Outro exemplo, a construção de narrativas e enquadramentos por parte de actores mal-intencionados tem-se revelado um desafio formidável, uma vez que estas táticas não só distorcem a realidade, como também minam a confiança nas instituições democráticas (Berger & Luckmann, 2003; Candelas, 2023), um elemento pouco abordado na resposta institucional espanhola, e onde apostas como a literacia digital ou os verificadores de factos (DSN, 2021) produzem resultados muito limitados. Luckmann, 2003; Candelas, 2023) um elemento pouco abordado na resposta institucional espanhola, e onde apostas como a literacia digital ou os *verificadores de factos* (DSN, 2021) produzem resultados muito limitados (Pennycook, Bear, Collins, & Rand, 2020; Flynn, Nyhan, & Reifler, 2017). De facto, as narrativas falsas e altamente enganadoras tendem a prevalecer devido

à sua capacidade de explorar as emoções humanas, como o medo e a indignação moral, o que aumenta o seu impacto e difusão nas redes sociais (Pennycook & Rand, 2021).

A análise da eficácia das estratégias propostas sugere que uma abordagem global que combine medidas técnicas e cognitivas é essencial para desenvolver uma resposta eficaz à desinformação. As estratégias actuais, embora necessárias, não conseguiram antecipar e responder às ameaças emergentes devido à sua abordagem reactiva (Badillo e Arteaga, 2024) e parcial que não aborda elementos-chave do problema, como as narrativas. Há uma clara necessidade de adotar uma postura mais proactiva e prospetiva, que permita às instituições não só responder às ameaças actuais, mas também antecipar e neutralizar futuras campanhas de desinformação (Libicki, 2021).

Uma das iniciativas propostas pelos principais intervenientes é a implementação de tecnologias avançadas, como a inteligência artificial e a aprendizagem automática, que podem desempenhar um papel crucial na identificação precoce de padrões de desinformação (NATO, 2021; INCIBE, 2024; DSN, 2024b; Comissão Europeia, 2025). Estas tecnologias permitem a análise em tempo real de grandes volumes de dados, facilitando a deteção de anomalias que podem indicar a presença de campanhas de desinformação coordenadas (Rodríguez Lorenzo et al., 2023). No entanto, como discutido ao longo deste artigo, para que estas ferramentas sejam eficazes, é essencial que sejam integradas num quadro institucional de defesa mais amplo que inclua tanto a cibersegurança como a defesa cognitiva.

Para além das medidas tecnológicas, a investigação sublinha a importância de reforçar tanto a sociedade como as suas instituições, aumentando a sua profundidade e capacidades estratégicas. A luta contra a desinformação exige um maior investimento em recursos económicos, institucionais e humanos (Rodríguez Lorenzo et al., 2023), proporcional à magnitude da ameaça. Incorporar a lógica da sociedade híbrida nas propostas estratégicas e táticas pode aumentar a sua eficácia e reduzir os custos de investimento na resposta (Arias Gil, 2020). Esta lógica permite uma maior adaptação às ameaças emergentes e uma resposta mais eficiente. É essencial que a Espanha desenvolva capacidades nacionais robustas, especialmente tendo em conta que a FIMI envolve não só grandes potências como a Rússia e a China, mas também uma variedade de actores (Badillo & Arteaga, 2024), para os quais a resposta não pode depender exclusivamente de organismos internacionais como a NATO ou a UE.

É necessário ultrapassar o paradigma centrado na promoção do pensamento crítico e da literacia mediática e avançar para um conceito semelhante ao proposto por Arias Gil de "cidadão estratégico" (2020). Esta nova abordagem implica transformar a lógica da responsabilidade individual, que é passiva, atomizada, parcial e de desenvolvimento a médio/longo prazo, numa resposta social mais proactiva, colectiva e coordenada. Em vez de depender apenas da formação individual em competências críticas, o cidadão estratégico é um recurso coletivo, proactivo, descentralizado (mas coordenado) que pode agir rapidamente face a ameaças de desinformação. Esta mudança de abordagem poderia permitir uma resposta mais dinâmica e eficaz, abordando as ameaças a curto prazo e facilitando uma maior adaptabilidade à evolução das táticas dos intervenientes na desinformação.

Uma recomendação fundamental é a necessidade de formação, simulações e manobras específicas no domínio da desinformação, à semelhança das realizadas noutros

domínios da segurança e da defesa. Esta proposta está ausente de toda a documentação analisada anteriormente. Estas actividades permitiriam que as instituições estivessem mais bem preparadas para identificar e neutralizar as campanhas de desinformação antes de estas causarem danos significativos. Além disso, propõe-se uma mudança para uma postura mais proactiva (utilização de comunicação estratégica) e prospetiva, que permita identificar potenciais vectores de ataque e tomar medidas preventivas para os minimizar, neutralizar ou atenuar antes de se tornarem ameaças reais. Isto inclui a incorporação da lógica assimétrica da sociedade híbrida, onde as respostas tácticas e estratégicas podem ser mais eficazes e menos dispendiosas (Arias Gil, 2020).

Por último, a criação de estruturas mais densas e coordenadas na luta contra a desinformação é apresentada como uma medida essencial. Isto inclui a formação de quadros intermédios da administração pública, do sector privado e da sociedade civil, especialmente em áreas relacionadas com a comunicação, a prospetiva e a análise sociopolítica. Essa formação é fundamental para garantir que todos os setores da sociedade estejam alinhados e preparados para enfrentar as complexas ameaças representadas pela desinformação (DSN, 2022). Nesse sentido, a disputa pelo controle dos quadros narrativos tornou-se um elemento central na luta contra a desinformação, onde o objetivo não é apenas combater as falsidades, mas também estabelecer quadros alternativos que reconfigurem o debate público (Tuñón Navarro, Oleart, & Bouza García, 2019). Do mesmo modo, conhecer, eliminar, mitigar ou neutralizar as próprias vulnerabilidades culturais, políticas ou sociais é fundamental para eliminar os vectores de ataque, reduzir as vulnerabilidades e aumentar a resiliência.

Em conclusão, é necessária uma mudança significativa na forma como Espanha lida com a desinformação. Não basta aplicar medidas técnicas ou reactivas; é essencial desenvolver uma estratégia global que reforce os aspectos sociais, cognitivos e tecnológicos, promovendo uma defesa mais coordenada, proactiva e adaptativa contra as ameaças de desinformação num ambiente híbrido global cada vez mais dinâmico e complexo.

9. REFERÊNCIAS BIBLIOGRÁFICAS

- Adame Hernández, J. F. (2024). España frente a la desinformación: Desafíos híbridos y respuestas convencionales (Dissertação de mestrado, Centro Universitário da Guarda Civil).
- Alastuey Rivas, J., García López, M. I., García Vizcaíno, F., Garrido López, A., Mora Moret, F., Pedrazo Majarrez, J. M., & Pérez-Tejada García, S. (2024). A desinformação como arma de guerra. Documento de opinião do IEEE 26/2024. Instituto Espanhol de Estudos Estratégicos (IEEE). Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEO26_2024_VVA_A_Desinforma (acedido em 06/04/2025).
- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), 211-236. <https://doi.org/10.1257/jep.31.2.211>(acedido em 06/04/2025).
- Allenby, B., & Garreau, J. (2017, 3 de janeiro). A narrativa armada é o novo espaço de batalha. *Defence One*. Recuperado de <http://bit.ly/3XyiwB2> (acedido em 14/08/2024).
- Althusser, L. (1971). *Ideologia e Aparelhos Ideológicos de Estado*. Medellín: La Oveja Negra. Recuperado de <https://lobosuelto.com/wp-content/uploads/2018/10/Althusser-L.-Ideolog%C3%ADa-y-aparatos-ideol%C3%B3gicos-de-estado.-Freud-y-Lacan-1970-ed.-Nueva-Visi%C3%B3n-1974.pdf> (acedido em 14/08/2024).
- Arias Gil, E. (2020). Insurgência de baixo custo: uma ameaça assimétrica emergente. Recuperado de <https://canal.uned.es/video/5f6b02325578f274ac7a0632> (acedido em 06/04/2025).
- Arias Gil, E. (2021). A dimensão emergente das notícias falsas: guerra centrada em redes e guerra memética. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Relatório. Instituto para o Desenvolvimento da Inteligência no Domínio do Terrorismo, Segurança e Defesa (IDITESDE). <https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> (acedido em 14/08/2024).
- Arteaga, Félix (2020). La lucha contra la desinformación: cambio de modelo. Real Instituto Elcano. <https://www.realinstitutoelcano.org/comentarios/la-lucha-contra-la-desinformacion-cambio-de-modelo> (acedido em 06/04/2025).
- Astorga González, L. (2020). A manipulação cognitiva no século XXI. *Revista del Instituto Español de Estudios Estratégicos*, 16, 15-44. Recuperado de <https://revista.ieee.es/article/view/2208> (acedido em 06/04/2025).
- Aznar Fernández-Montesinos, F. (2021). A batalha das narrativas. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Relatório. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE).

<https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> (acedido em 14/08/2024).

Badillo, Á. M., & Arteaga, F. (2024). O impacto estratégico da desinformação em Espanha. Relatório Iberifier. Recuperado de <https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estrategico-de-la-desinformacion-en-espana.pdf> (acedido em 06/04/2025).

BBC Mundo (16 de fevereiro de 2018). Departamento de Justiça dos EUA acusa 13 cidadãos russos de interferir na eleição presidencial de 2016. <https://www.bbc.com/mundo/noticias-internacional-43092239> (acessado em 04/04/2025).

Bennett, W. L., & Livingston, S. (2020). A ordem da desinformação: comunicação disruptiva e o declínio das instituições democráticas. Revista Europeia de Comunicação. Recuperado de <https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/downloads/The%20Disinformation%20Order%3B%20Livingston.pdf> (acedido em 14/08/2024).

Berger, P. L., & Luckmann, T. (1966). A construção social da realidade. Buenos Aires. Recuperado de <https://redmovimientos.mx/wp-content/uploads/2020/07/La-Construcci%C3%B3n-Social-de-la-Realidad-Berger-y-Luckmann.pdf> (acedido em 06/04/2025).

Burkhardt, J. M. (2017). História das notícias falsas. Library Technology Reports, 53(8), 5-9. <https://journals.ala.org/index.php/ltr/article/view/6497/8631> (acedido em 06/04/2025).

Buvarp, P. M. H. (2021). O espaço de influência: desenvolvimento de um novo método para concetualizar a manipulação de informação estrangeira e a interferência nas redes sociais. Estabelecimento Norueguês de Investigação em Defesa (FFI). Recuperado de <https://www.ffi.no/en/publications-archive/the-space-of-influence-developing-a-new-method-to-conceptualise-foreign-information-manipulation-and-interference-on-social-media> (acedido em 02/06/2025).

Calvo Albero, J. L. (18 de dezembro de 2017). Desinformação: velhas ideias em novos formatos. Estratégia Global. <https://global-strategy.org/desinformacion-viejas-ideas-en-nuevos-formatos> (acedido em 06/04/2025).

Calvo, J. L. (abril de 2023). Da guerra silenciosa à guerra híbrida. Revista Española de Defensa. <https://www.defensa.gob.es/Galerias/gabinete/red/2023/04/p-54-57-red-404-desinformacion.pdf> (acedido em 06/04/2025).

Candelas, M. (2023). Propaganda em conflitos geopolíticos: da guerra psicológica à guerra além fronteiras. IEEE Opinion Paper 02/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEE002_2023_MIG_CAN_Propaganda.pdf (acedido em 06/04/2025).

- Caridad-Sebastián, M, Morales-García, A. M., Martínez-Cardama, S, & García López, F (2018). Infomediação e pós-verdade: O papel das bibliotecas. https://e-archivo.uc3m.es/bitstream/handle/10016/28096/Infomediacion_EPI_2018.pdf?sequence=1&isAllowed=y (acedido em 20/08/2024).
- Castro Torres, J. I. (2021). O ambiente de desinformação e a construção de narrativas. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Relatório. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). <https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> [URL não disponível] (acedido em 14/08/2024).
- CCN-CERT. (2019, 11 de novembro). ELISA: Nova ferramenta de vigilância cibernética do CCN-CERT. Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Noviembre/Noticia-2019-11-11-ELISA-nueva-herramienta-de-cibervigilancia-del-CCN-CERT.html?idioma=es (acedido em 06/04/2025).
- Centro de Investigações Sociológicas (CIS) (Centro de Investigação Sociológica). 2021. Barómetro CIS de febrero-julio de 2022. Madrid, Espanha. Recuperado de <https://www.cis.es/documents/d/cis/es3351marpdf> (acedido em 14/08/2024).
- Centro de Investigaciones Sociológicas (CIS) (2023). Estudio 3424: Perceção social dos aspectos científicos da manipulação genética e da biotecnologia. Recuperado de <https://www.cis.es/es/detalle-ficha-estudio?origen=estudio&codEstudio=3424> (acedido em 14/08/2024).
- Centro de Investigaciones Sociológicas (CIS) (2024). Estudio 3486: Inquérito sobre Tendências Sociais (IV). Recuperado de https://www.cis.es/visor?migrado=false&fichero=cru3486_enlace (acedido em 01/06/2025).
- Chan, R. (2020). O denunciante da Cambridge Analytica explica como a empresa utilizou os dados do Facebook para influenciar as eleições. <https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10> (acedido em 06/04/2025).
- Chomsky, N. (1992). *Necessary illusions*. Recuperado de https://resistir.info/livros/chomsky_ilusiones_necesarias.pdf (acedido em 06/04/2025)
- Clausewitz, C. von. (1976). Sobre a guerra. Esfera dos Livros. Recuperado de <https://www.esferalibros.com/wp-content/uploads/2022/09/De-la-guerra-primeras.pdf> (acedido em 14/08/2024).
- Colom, G. (2018). Guerras híbridas. Quando o contexto é tudo. Revista do Exército. Recuperado de <https://www.ugr.es/~gesi/Guerras-hibridas.pdf> (acedido em 20/08/2024).

- Colom, G. (2018b). A doutrina Gerasimov e o pensamento estratégico russo contemporâneo. *Revista do Exército*. Recuperado de <https://www.thiber.org/2019/05/11/la-doctrina-gerasimov-y-el-pensamiento-estrategico-ruso-contemporaneo> (acedido em 06/04/2025).
- Comissão Europeia (2022). Código de Conduta Reforçado sobre Desinformação. Obtido em <https://ec.europa.eu/newsroom/dae/redirection/document/87585> (acedido em 20/08/2024).
- Comissão Europeia (2024, 17 de dezembro). A Comissão dá início a um processo formal contra o TikTok devido a riscos eleitorais ao abrigo da Lei dos Serviços Digitais Retrieved from https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487 (accessed 22/03/2025).
- Comissão Europeia (2025, 15 de abril). Comissão investe 140 milhões de euros na implantação de tecnologias digitais essenciais. Obtido em https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/la-comision-invierte-140-millones-de-euros-para-desplegar-tecnologias-digitales-clave-2025-04-15_es#:~:text=La%20Comisi%C3%B3n%20ha%20lanzado%20cuatro,y%20luchar%20contra%20la%20desinformaci%C3%B3n (acedido em 22/03/2025).
- Dahlgren, P. (2018). *Media, conhecimento e confiança: O aprofundamento da crise epistémica da democracia*. Javnost - O Público, 25(1-2), 20-27. Recuperado de <https://doi.org/10.1080/13183222.2018.1418819> (acedido em 06/04/2025).
- Davis, G. (2005). A ideologia do visual. Em M. Rampley (Ed.), *Exploring visual culture: Definitions, concepts, contexts* (pp. 163-178). Edinburgh University Press.
- Painel de controlo DESI para a Década Digital (2024). Painel de controlo DESI para a Década Digital. Comissão Europeia. Obtido em <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts> (acedido em 06/04/2025).
- DSN (2021). *Estratégia de Segurança Nacional*. Departamento de Segurança Interna (2021).
- DHS (2022). Departamento de Segurança Interna (2022). Recuperado de <https://www.dsn.gob.es/sites/default/files/documents/LibroDesinfoSN.pdf> (acedido em 14/08/2024).
- DSN (2023a). Fórum contra as campanhas de desinformação no domínio da segurança nacional - Jobs 2023. Obtido em <https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf> (acedido em 14/08/2024).
- DSN (2023b). Apresentação do trabalho 2023: Fórum contra as campanhas de desinformação no domínio da segurança nacional. Obtido em <https://www.dsn.gob.es/es/actualidad/sala-prensa/presentaci%C3%B3n-trabajos->

2023-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito (acedido em 14/08/2024).

DHS. Departamento de Segurança Interna (2024). Relatório Anual de Segurança Nacional 2023. Governo de Espanha. Recuperado de https://www.newtral.es/wp-content/uploads/2024/03/IASN2023_0.pdf (acedido em 14/08/2024).

DHS. Departamento de Segurança Interna (2024b). Trabalho do Fórum contra Campanhas de Desinformação - Iniciativas 2024. Obtido em <https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/trabajos-foro-contra-campanas-desinformacion-iniciativas-2024#:~:text=medios%20de%20comunicaci%C3%B3n.-,Trabajos%20del%20Foro%20contra%20las%20Campa%C3%B1as%20de%20Desinformaci%C3%B3n%20%2D%20Iniciativas%202024,-Accesible> (acedido em 14/08/2024).

Donoso Rodríguez, D. (2020). *Implicações do domínio cognitivo nas operações militares*. Revista IEEE, 01/2020. Recuperado de https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf (acedido em 01/06/2025).

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: the moderating effect of political interest and diverse media. *Informação, Comunicação e Sociedade*. Recuperado de <https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract> (acedido em 06/04/2025).

SEAE (Serviço Europeu para a Ação Externa) (2024). 2º relatório sobre ameaças FIMI - janeiro de 2024. Retirado de https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (acedido em 14/08/2024).

SEAE, Serviço Europeu para a Ação Externa (2015). Tackling disinformation, foreign information manipulation & interference. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (acedido em 14/08/2024).

ENISA E SEAE. (2022). Manipulação e interferência de informações estrangeiras (FIMI) e cibersegurança - cenário de ameaças. Obtido em https://www.cde.ual.es/wp-content/uploads/2022/12/EEAS-ENISA-Disinformation_Misinformation.pdf (acedido em 14/08/2024).

Eurobarómetro (2024). EUROBARÓMETRO NORMA 102 Opinião Pública na União Europeia. Comissão Europeia. Recuperado de <https://europa.eu/eurobarometer/surveys/detail/3215> (acedido em 14/08/2024).

IFJ, Federação Internacional de Jornalistas (2018). O que são notícias falsas? Um guia para combater a desinformação na era da pós-verdade. Recuperado de

https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf
(acedido em 06/04/2025).

Flores, J. M. (2022). "Notícias falsas sempre existiram, mas hoje foram catapultadas pelas redes sociais". Recuperado de <https://www.ucm.es/otri/noticias-las-fake-news-siempre-han-existido-pero-hoy-en-dia-se-han-visto-catapultadas-por-las-redes-sociales> (acedido em 20/08/2024).

Flynn, D., Nyhan, B., & Reifler, J. (2017). The nature and origins of misperceptions: understanding false and unfounded beliefs about politics. *Political Psychology*, 38(6), 1053-1077. <https://doi.org/10.1111/pops.12394> (acedido em 06/04/2025).

Foucault, M. (1972). *A arqueologia do saber*. Siglo XXI Editores. Recuperado de https://monoskop.org/images/b/b2/Foucault_Michel_La_arqueologia_del_saber.pdf

(acedido em 14/08/2024).

Garrós Font, I., & Santos Silva, M. F. (2021). A luta contra a infodemia: Análise do procedimento de ação contra a desinformação. *Revista de Comunicação e Saúde*, 11(2), 75-89. [https://doi.org/10.35669/rcys.2021.11\(2\).75-89](https://doi.org/10.35669/rcys.2021.11(2).75-89)

Gelfert, Axel (2018). Notícias falsas: uma definição. *Informal Logic*, 38. Recuperado de https://informallogic.ca/index.php/informal_logic/article/view/5068 (acedido em 06/04/2025).

Goffman, E. (2006). *Frame analysis: The frames of experience*. Centro de Investigação Sociológica.

Gómez, A. (2020, 19 de novembro). O novo procedimento de ação contra a desinformação: A controvérsia é servida. Blog de Propiedad Intelectual y NNTT Garrigues. Recuperado de <https://blogip.garrigues.com/publicidad/el-nuevo-procedimiento-de-actuacion-contrala-desinformacion-la-polemica-esta-servida> (acedido em 06/04/2025).

Hafen, R. (2024). A arte operacional chinesa: o primado da dimensão humana. *Military Review*. Retirado de <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Q2-2024/Hafen-SPA-Q2-2024/Hafen-SPA-Q2-2024-UA.pdf> (acedido em 14/08/2024).

Herman, E. S., & Chomsky, N. (1988). Os guardiões da liberdade. Recuperado de <https://www.labiblioteca.mx/llyfrgell/1783.pdf> (acedido em 06/04/2025).

Hernández-García, L. A. (2022). A zona cinzenta: uma abordagem concetual a partir da FAS. Recuperado de <https://www.atalayar.com/opinion/luis-hernandez-garcia-ieee/la-zona-gris-una-aproximacion-concetual-desde-las-fas/20220412121331136376.html> (acedido em 06/04/2025).

Hoffman, F. (2009). Hybrid warfare and challenges (Guerra híbrida e desafios). *Small Wars Journal*. Recuperado de

<https://smallwarsjournal.com/documents/jfqhoffman.pdf> (acedido em 06/04/2025).

INCIBE (2024). DANGER: Cibersegurança para deteção, análise e filtragem de conteúdos falsos ou maliciosos em ambientes hiperconectados. Recuperado de <https://www.incibe.es/node/521663> (acedido em 06/04/2025).

Jamieson, K. H., & Cappella, J. N. (2008). *Echo chamber: Rush Limbaugh and the conservative media establishment*. Oxford University Press.

Jordán, J. (2018). Conflito internacional na zona cinzenta: uma proposta teórica a partir da perspetiva do realismo ofensivo. *Revista Española de Ciencia Política*, n.º 48. Retrieved from <https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf>

(acedido em 20/08/2024).

Juurvee, I., & Mattiisen, M. (agosto de 2020). A crise do soldado de bronze de 2007: Revisitando um caso inicial de conflito híbrido. Centro Internacional de Defesa e Segurança. Recuperado de <https://bit.ly/3iRyeZe> (acedido em 06/04/2025).

Latam Chequea (2022). Notícias falsas sobre COVID-19 verificadas pela rede Latam Chequea. Recuperado de <https://chequeado.com/investigaciones/como-la-desinformacion-sobre-covid-19-infecto-a-america-latina> (acedido em 14/08/2024).

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Rothschild, D. (2018). A ciência das notícias falsas: uma agenda de pesquisa. *Science*, 359(6380), 1094-1096. Recuperado de <https://doi.org/10.1126/science.aao2998> (acedido em 14/08/2024).

Libicki, M. C. (2021). O ciberespaço na paz e na guerra. Imprensa do Instituto Naval. Recuperado de https://www.researchgate.net/publication/343399173_Military_Operations_in_Cyberspace (acedido em 06/04/2025).

Lupiáñez Lupiáñez, M. (2023). Como lidar com um ataque cognitivo: deteção de protótipos de propaganda e manipulação em operações psicológicas dirigidas a civis durante um conflito. *Revista del Instituto Español de Estudios Estratégicos*, (22), 61-93. Obtido em <https://revista.ieee.es/article/view/6058> (acedido em 14/08/2024).

MAEUEC, Ministério dos Negócios Estrangeiros, da União Europeia e da Cooperação (2021). *Estratégia de Ação Externa 2021-2024*. Retirado de <https://www.exteriores.gob.es/estrategia2021-2024.pdf> (acedido em 14/08/2024).

Maggioni, M., & Magri, P. (2018). Twitter e Jihad: A estratégia de comunicação do ISIS. *Revista de Estudos do Ciberespaço*, 2(2), 239-241. Recuperado de <https://doi.org/10.22059/jcss.2018.66728> (acedido em 14/08/2024).

- Maldita.es (2023). O que é o prebunking? É assim que esta técnica funciona contra a desinformação antes que ela se espalhe. Recuperado de <https://maldita.es/nosotros/20230323/prebunking-que-es-antes-desmentido> (acedido em 06/04/2025).
- Marchal González, A. N. (2023). A necessidade de um novo tipo de crime: a desinformação como ameaça à ordem pública. *Boletín Criminológico*, 1(2023), 1-14. Recuperado de <https://revistas.uma.es/index.php/boletin-criminologico/article/view/17222/17250> (acedido em 06/04/2025).
- Martín Renedo, S. (2022). Zonas cinzentas no terreno: o fim das guerras convencionais? Documento de opinião do IEEE 93/2022. Obtido em https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEO93_2022_SAU_MAR_Zonas.pdf (acedido em 06/04/2025).
- Mayoral, J, Parratt, S, & Morata, M. (2019). Desinformação jornalística, manipulação e credibilidade: uma perspetiva histórica. *História e Comunicação Social*, 24(2), 395-409. Recuperado de <https://revistas.ucm.es/index.php/HICS/article/view/66267> (acedido em 06/04/2025).
- McCuen, J. (2008). Hybrid Wars [Guerras Híbridas]. *Military Review*, 88(2), 107-113. Obtido em https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf (acedido em 06/04/2025).
- McIntyre, L. (2018). *Posverdad*. Madrid: Cátedra.
- MPJRC. Ministério da Presidência, da Justiça e das Relações com os Tribunais (2024). Plano de ação para a democracia. Retirado de https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (acedido em 06/04/2025).
- Newtral (2022). Campeonato do Mundo de Futebol do Qatar, uma montra de boatos e desinformação. Recuperado de <https://www.newtral.es/bulos-mundial-catar/20221203> (acedido em 06/04/2025).
- Novoa-Jaso, M. F., Sierra, A., Labiano, R., & Vara-Miguel, A. (2024). Relatório de notícias digitais Espanha 2024. Qualidade jornalística e pluralidade: chaves para a confiança nas notícias na era da inteligência artificial (IA). Servicio de Publicaciones de la Universidad de Navarra. Recuperado de https://www.unav.edu/documents/98033082/0/DNR_2024.pdf (acedido em 14/08/2024).
- OCDE (2024), Facts versus falsehoods: Strengthening democracy through information integrity, OCDE. Publishing, Paris. Obtido em <https://doi.org/10.1787/06f8ca41-es> (acedido em 14/08/2024).

- Olmo, J. A. (2019). Desinformação: conceito e perspectivas. Real Instituto Elcano. Recuperado de <https://www.realinstitutoelcano.org/analysis/desinformacion-concepto-y-perspectivas> (acedido em 06/04/2025).
- OMS, Organização Mundial de Saúde (2020). Gerir a infodemia da COVID-19: Promover comportamentos saudáveis e mitigar os danos da desinformação. Obtido em <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation> (acedido em 14/08/2024).
- Despacho PCM/1030/2020, de 30 de outubro, que publica o Procedimento de atuação contra a desinformação aprovado pelo Conselho de Segurança Nacional (2020). *Diário da República*. Retirado de <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-13663> (acedido em 14/08/2024).
- Despacho PJC/248/2025, de 13 de março, que publica o Acordo do Conselho de Segurança Nacional de 28 de janeiro de 2025, que aprova o procedimento para a elaboração da Estratégia Nacional contra as Campanhas de Desinformação (2025). *Diário da República*. Retirado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151
- NATO (2021, 12 de agosto). Combater a desinformação: melhorar a resiliência digital da Aliança. Obtido em <https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html> (acedido em 14/08/2024).
- NATO, Quartel-General (2024). Ameaças híbridas e guerra híbrida: currículo de referência. Obtido em https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (acedido em 14/08/2024).
- PDC-01. Publicação Doutrinária Conjunta PDC-01 (A) Doutrina para o emprego das Forças Armadas. Estado-Maior da Defesa, 2018. Recuperado de <https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html> (acedido em 14/08/2024).
- Pennycook, G., & Rand, D. G. (2021). A psicologia das notícias falsas. Tendências em Ciências Cognitivas, 25(5), 388-402. Recuperado de [https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613\(21\)00051-6](https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(21)00051-6) (acedido em 06/04/2025).
- Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). Fighting misinformation on social media using crowdsourced judgments of news source quality (Combater a desinformação nas redes sociais utilizando julgamentos de fontes de notícias de qualidade). *Proceedings of the National Academy of Sciences*, 117(7), 2775-2785. <https://www.pnas.org/doi/abs/10.1073/pnas.1806781116> (acedido em 02/06/2025).

- Posetti, J., & Matthews, A. (2018). Um pequeno guia para a história das "notícias falsas" e da desinformação. Centro Internacional para Jornalistas. Recuperado de https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf (acedido em 06/04/2025).
- Quiñones de la Iglesia, F. J. (2021). Desinformação e subversão (2.0): as técnicas da Guerra Fria reaparecem no domínio da informação do século XXI. Documento de referência do IEEE 12/2021. Recuperado de https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM12_2021_FRAQUI_Desinformacion.pdf (acedido em 06/04/2025).
- Instituto Reuters para o Estudo do Jornalismo (2024). Digital News Report 2024. Universidade de Oxford. Recuperado de <https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024> (acedido em 06/04/2025).
- Rid, T. (2021). Desinformação e guerra política. Barcelona: Crítica.
- Rodrigo Alsina, M. (2005). La construcción de la noticia. Recuperado de <https://www.um.es/tic/LIBROS%20FCI-I/La%20produccion%20de%20la%20noticia.pdf> (acedido em 20/08/2024).
- Rodríguez Lorenzo, E, Morales, R, Crescente, D, Cabello, M. I, & Paz, I. (2023). Inteligência artificial na guerra híbrida como arma de desinformação. Documento de opinião do IEEE. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEE061_2023_EDU ROD_Inteligencia.pdf (acedido em 06/04/2025).
- Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). A inoculação psicológica melhora a resiliência contra a desinformação nas redes sociais. *Science Advances*, 8. Recuperado de <https://www.science.org/doi/10.1126/sciadv.abo6254> (acessado em 06/04/2025).
- Sartori, G. (2007). Política. Lógica y métodos en las ciencias sociales. Fondo de Cultura Económica. Recuperado de <https://maestriainap.diputados.gob.mx/documentos/materia1/sem1/02.pdf> (acedido em 06/04/2025).
- SEAE. (2023). Luta contra a desinformação: Manipulação e interferência de informações estrangeiras (FIMI). Obtido em https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (acedido em 14/08/2024).
- Tandoc, E. C., Jr., Lim, Z. W., & Ling, R. (2018). Definindo notícias falsas: uma tipologia de definições acadêmicas. *Jornalismo Digital*, 6(2), 137-153. Recuperado de <https://doi.org/10.1080/21670811.2017.1360143> (acedido em 06/04/2025).
- Terán, E. (2019). Desinformação na UE: ameaça híbrida ou fenómeno comunicativo? Evolução da estratégia da UE desde 2015

<https://www.idee.ceu.es/Portals/0/Desinformaci%C3%B3n%20en%20la%20UE.pdf> (acedido em 06/04/2025).

- Torres, C. M. (2021). Fake news: a influência da pós-verdade e da desinformação na política contemporânea. *Comunicação e Sociedade*, 18(2), 199-217. Recuperado de <https://revistas.javeriana.edu.co/index.php/comunicacionysociedad/article/view/31487> (acedido em 14/08/2024).
- Torres-Soriano, M. R. (2022). Operações de influência vs. desinformação: diferenças e pontos de ligação. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEEO64_2022_MANTOR_Operaciones.pdf (acedido em 01/06/2025).
- Supremo Tribunal de Justiça (2021, 18 de outubro). Sentencia STS 1238/2021. Recuperado de <https://vlex.es/vid/877507365> (acedido em 14/08/2024).
- Tuñón Navarro, J., Oleart, Á., & Bouza García, L. (2019). Actores Europeus e Desinformação: a disputa entre fact-checking, agendas alternativas e geopolítica. *Revista de Comunicação e Cidadania Digital*, 8(1), 223-238. Recuperado de <https://www.redalyc.org/journal/5894/589466348012> (acedido em 06/04/2025).
- Walker, R. G. (1998). *Spec Fi: The United States Marine Corps and Special Operations*. Monterey, Naval Postgraduate School. Recuperado de <https://apps.dtic.mil/sti/pdfs/ADA359694.pdf> (acedido em 14/08/2024).
- Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Conselho da Europa. Recuperado de <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-resear/168076277c> (acedido em 14/08/2024).



Artigo de investigação

A INTELIGÊNCIA EM FOCO: DA TEORIA CLÁSSICA A UMA NOVA ABORDAGEM DE IMPLEMENTAÇÃO NA ERA DIGITAL

Tradução para o português com ajuda de IA (DeepL)

Paula Castro Castañer

Perito em segurança na Telefónica S.A.

Doutorando em Ciências Forenses na Universidade de Alcalá

Mestrado em Cibersegurança e Privacidade pela Universitat Oberta de Catalunya (UOC)

paula.castroc@edu.uah.es

ORCID: 0009-0008-0315-8387

Recebido a 14/02/2025

Aceite em 16/06/2025

Publicado em 27/06/2025

Citação recomendada: Castro P. (2025). A inteligência em foco: Da teoria clássica a uma nova abordagem de implementação na era digital. *Revista Logos Guardia Civil*, 3(2), p.p. 71-100.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

DEDICAÇÃO

*Ao meu tutor, Hilário, por ter confiado em
mim e me ter apoiado em todos os meus
projectos.*

A INTELIGÊNCIA EM FOCO: DA TEORIA CLÁSSICA A UMA NOVA ABORDAGEM DE IMPLEMENTAÇÃO NA ERA DIGITAL

Resumo: INTRODUÇÃO. 1.1. NOTA METODOLÓGICA. 2. CONCEITO E EVOLUÇÃO DA INTELIGÊNCIA. 2.1. TIPOS DE INTELIGÊNCIA. 2.2. EVOLUÇÃO DAS ABORDAGENS E ESTRATÉGIAS DE INTELLIGENCE. 3. O CICLO DE INTELLIGENCE. 4. PROPOSTA DE ACTUALIZAÇÃO DO CICLO DE INTELLIGENCE NA ERA DIGITAL: O MODELO IDEM. 4.1. EXEMPLO PRÁTICO DE APLICAÇÃO DO MODELO IDEM. 5. CONCLUSÕES 6. 5. CONCLUSÕES 6. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: Este artigo aborda a evolução da intelligence no domínio da Defesa e Segurança, desde as abordagens tradicionais até à sua adaptação à era digital, estabelecendo uma proposta que responde a algumas das limitações apontadas na literatura sobre o ciclo clássico de intelligence. Para o efeito, são explorados conceitos-chave, como a definição do conceito de intelligence, os diferentes tipos de intelligence e ainda o ciclo tradicional de intelligence e as suas fases. Além disso, é apresentada uma revisão da evolução e das diferentes abordagens que foram adoptadas ao longo da história no domínio da inteligência. Por fim, propõe um modelo de inteligência, denominado IDEM, com fases flexíveis e que combina o talento do analista humano e o processamento automatizado de big data para garantir uma inteligência proactiva, adaptativa e de qualidade face às complexas ciberameaças transnacionais.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Palavras-chave: ciberameaças, ciberinteligência, ciclo de inteligência, modelo IDEM, abordagem em rede

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red .

ABREVIATURAS

ABI: *Inteligência baseada em atividades*

CCN-CERT: Centro Nacional de Criptologia - *Equipa de Resposta a Emergências Informáticas*

CESID: Centro Superior de Informação da Defesa (Centro de Informação da Defesa)

CIA: *Agência Central de Inteligência, Agência Central de Inteligência*

CIFAS: Centro de Inteligência das Forças Armadas

CNI: Centro Nacional de Informações

COMINT: *Informações sobre comunicações*

COP: *Policiamento comunitário, policiamento orientado para a comunidade*

CTI: *Informação sobre ameaças cibernéticas, Informação sobre ameaças cibernéticas*

CYBINT: Ciberespionagem, Ciberespionagem

ELINT: *Inteligência eletrónica*

FISINT: *Informações de sinais de instrumentação estrangeira*

GEOINT: *Inteligência Geoespacial, Inteligência Geoespacial*

HUMINT: *Inteligência Humana*

IDEM: Enhanced Dynamic Intelligence Enrichment and Enhancement (enriquecimento e melhoramento da inteligência dinâmica)

IDS: *Sistema de Detecção de Intrusão, Sistema de Detecção de Intrusão*

ILP: *Intelligence-Led Policing, Policiamento liderado por informações*

IMINT: *Inteligência imagiológica*

ISR: *Intelligence Surveillance and Reconnaissance*), *Informações, vigilância e reconhecimento*

JISR: *Joint Intelligence Surveillance and Reconnaissance* (*Informações, Vigilância e Reconhecimento Conjuntos*), *Informações, Vigilância e Reconhecimento Conjuntos*

MASINT: *Inteligência de Medição e Assinatura*

ML: *Aprendizagem automática, Aprendizagem automática*

NLP: *Processamento de linguagem natural*

OSCE: *Organização para a Segurança e a Cooperação na Europa, Organização para a Segurança e a Cooperação na Europa*

OSINT: *Informações de fonte aberta*

SCADA: *Controlo de Supervisão e Aquisição de Dados*

SECED: *Serviço Central de Documentação*

SIEM: *Gestão de Informações e Eventos de Segurança*

SIGINT: *Inteligência de sinais*

SOCMINT: *Inteligência em matéria de redes sociais, Inteligência em matéria de redes sociais*

TCPED: *Atribuição, recolha, processamento, exploração, difusão, abordagem, recolha, processamento, exploração, difusão*

TTPs: *Ameaças, Técnicas e Procedimentos*

1. INTRODUÇÃO

Num mundo em que a Inteligência Artificial parece dominar grande parte das atenções e preocupações públicas, onde é que a inteligência, em todas as suas outras formas, fica em segundo plano? A omnipresença da Inteligência Artificial nos debates contemporâneos ofusca frequentemente a importância de outros tipos de inteligência que são fundamentais para o progresso e o desenvolvimento humanos.

A inteligência humana, nas suas múltiplas manifestações, continua a ser um pilar insubstituível para a prosperidade da sociedade, ainda mais nos contextos complexos e mutáveis desta Era Digital. Uma dessas manifestações é a inteligência competitiva, que permite obter recomendações acionáveis através do processamento de informações sobre o ambiente externo em busca de oportunidades ou desenvolvimentos que possam ter impacto na posição competitiva de uma empresa ou país (Lee, 2023). Ou a inteligência prospetiva, que, com base em informações passadas e presentes, bem como em especulações futuras, tenta "desenhar" um mapa cognitivo para determinar diferentes opções e reduzir o nível de incerteza que acompanha qualquer decisão (Montero Gómez, 2006).

É verdade que o crescimento exponencial da digitalização, da exposição e da globalização está a impulsionar a origem e a evolução de novas formas de inteligência em resposta a novas tecnologias e métodos de recolha de dados, dando origem a inteligências como a inteligência de fonte aberta (OSINT) ou a inteligência geoespacial (GEOINT), entre outras. Estas disciplinas tiram partido da vasta quantidade de informação disponível para fornecer uma visão global, integrada e detalhada de vários fenómenos. No entanto, a inteligência não se deve limitar à recolha e análise de dados, mas deve também integrar considerações éticas e avaliar as potenciais consequências a longo prazo das decisões.

Atualmente, a informação e a tecnologia são vitais para quase todos os aspectos da vida, e a inteligência desempenha um papel crucial, especialmente no domínio da cibersegurança, uma vez que a capacidade de antecipar, identificar e atenuar as ameaças é essencial para preservar a integridade, a confidencialidade e a disponibilidade dos sistemas.

No entanto, coloca-se a questão: será esta capacidade uma realidade nas agências governamentais e privadas actuais, será a intelligence eficaz na antecipação e mitigação dos riscos crescentes no ciberespaço e estará o ciclo de intelligence atualizado para responder às exigências da Era Digital? O presente documento tem como objetivo realizar uma análise teórica para responder a estas questões e avaliar a eficácia da inteligência no contexto atual.

1.1. NOTA METODOLÓGICA

Para o desenvolvimento deste trabalho, foi realizada uma revisão narrativa da literatura académica e técnica relacionada com a inteligência nos domínios da defesa e segurança, bem como a sua adaptação ao ambiente digital. Esta revisão serviu de base para contextualizar a evolução do conceito, analisar criticamente o ciclo clássico de inteligência e fundamentar a proposta do modelo IDEM.

A pesquisa foi efectuada em bases de dados académicas como Scopus, Google Scholar e Dialnet, bem como em fontes institucionais nacionais e internacionais. Foram utilizadas palavras-chave em espanhol e inglês, tais como "ciclo de inteligência", "ciberinteligência", "inteligência de ciberameaças" ou "ciberameaças". Foi dada prioridade a publicações recentes (2000-2024) que oferecessem abordagens teóricas, modelos metodológicos ou análises críticas do processo de inteligência. Ocasionalmente, devido à falta de literatura de fonte aberta, foram consultados sítios Web de renome ou sítios Web escritos por especialistas técnicos na matéria.

Foram excluídos os documentos sem suporte académico ou institucional, bem como os textos que não abordavam especificamente a dimensão estrutural ou processual da inteligência. A literatura selecionada foi organizada em torno de cinco eixos temáticos: (1) definição do conceito de inteligência, (2) classificação dos tipos de inteligência, (3) evolução histórica e organizacional dos serviços de inteligência, (4) revisão crítica do ciclo tradicional e (5) propostas contemporâneas para sua adaptação à era digital.

Esta abordagem metodológica permitiu detetar lacunas teóricas relevantes e servir de base para o desenvolvimento de um modelo atualizado que integra tanto a dimensão humana como as capacidades tecnológicas da inteligência atual.

2. CONCEITO E EVOLUÇÃO DA INTELIGÊNCIA

O termo inteligência é um conceito abstrato e complexo de delimitar devido à multiplicidade de abordagens sob as quais pode ser estudado. Esta dificuldade não responde apenas à diversidade de domínios que a analisam, mas também aos desafios que se colocam num mesmo contexto para estabelecer uma definição única.

No domínio da defesa e da segurança, a maioria dos autores associa o nascimento da inteligência à emergência dos Estados e das relações interestatais. No entanto, não existe consenso sobre a definição de intelligence, em grande parte devido às diferentes abordagens adoptadas na prática por diferentes países (Andric & Terzic, 2023). Esta disparidade dificulta tanto o avanço teórico do seu estudo como a compreensão aprofundada das várias dimensões e factores que afectam a sua prática (Payá-Santos, 2023).

Neste contexto, uma das primeiras classificações fundamentais, a trindade, foi estabelecida por Sherman Kent, definindo três realidades para este conceito: a inteligência como organização, como processo e como resultado (Díaz Fernández, 2013).

- **Inteligência como organização:** refere-se aos serviços de inteligência principalmente sob a égide da administração pública, como é o caso do Centro Nacional de Inteligência (CNI) e do Centro de Inteligência das Forças Armadas (CIFAS) em Espanha. As funções destas instituições incluem a obtenção, avaliação, interpretação e difusão de informações para proteger e promover os interesses de Espanha, tanto dentro como fora do país; prevenir, detetar e neutralizar ameaças à Constituição, aos direitos e liberdades, à soberania, à segurança do Estado, à estabilidade institucional e ao bem-estar da população; promover a cooperação com serviços de informações estrangeiros e organizações internacionais; interpretar o tráfego de sinais estratégicos; coordenar a utilização de meios de encriptação; garantir a segurança da informação classificada; e

proteger as suas próprias instalações, informações e recursos (Jefatura del Estado, 2002).

- **Inteligência como processo:** compreende todas as atividades, geralmente englobadas no chamado ciclo de inteligência (discutido em maior profundidade em secções posteriores), que são necessárias para atender às demandas dos líderes e que interpretam um ambiente, contexto ou problema. Estas actividades são consideradas um processo cíclico contínuo e vão desde a recolha de informação de várias fontes, continuando com a sua posterior análise e processamento, até à disseminação dos dados de interesse para os utilizadores finais (Chainey & Chapman, 2013).
- **Inteligência como produto:** refere-se ao resultado e/ou conhecimento obtido, em qualquer formato, após o ciclo de inteligência. Esse produto deve influenciar a tomada de decisão e impactar o contexto interpretado (Chainey & Chapman, 2013).

Recentemente, foi também proposta uma quarta dimensão: **a inteligência como cultura**, definida por Navarro como "o conjunto de iniciativas e recursos que promovem a consciencialização da sua necessidade e proporcionam uma compreensão cívica da sua realidade" (Payá-Santos, 2023).

Independentemente da interpretação adoptada, a inteligência visa reduzir a incerteza intrínseca à condição humana e a complexidade do mundo contemporâneo na tomada de decisões para prevenir e evitar qualquer perigo ou ameaça (Jordan, 2015).

Para o conseguir, a inteligência baseia-se em conhecimentos teóricos relacionados com a política, a economia, as relações internacionais, a segurança, a sociologia, a tecnologia, a psicologia, etc. Por conseguinte, é essencial apresentar equipas de peritos de elevada qualidade nas diferentes áreas temáticas, a fim de abordar os problemas de múltiplas perspectivas e encontrar soluções mais eficazes com uma abordagem transversal.

O recente aspeto multidisciplinar da inteligência é uma consequência do alargamento do conceito de segurança e da crescente complexidade do contexto societal, onde as ameaças assimétricas e a ciberguerra são cada vez mais comuns.

Em contrapartida, uma das qualidades mais antigas dos serviços secretos é o secretismo das suas actividades e das informações obtidas. No entanto, a utilização crescente de fontes abertas (OSINT) está a mudar esta perspetiva. Além disso, a globalização e a expansão da utilização da Internet também afectam os conflitos, que são cada vez mais transnacionais e exigem uma cooperação internacional em matéria de informações. No entanto, a proteção das fontes, especialmente das fontes humanas (HUMINT), continua a ser um princípio fundamental, assim como a necessidade de preservar a discrição no tratamento das informações para evitar contramedidas, desinformação ou violação de operações sensíveis.

Em suma, pode-se estabelecer que a inteligência engloba o processo, o produto e a instituição que realiza a coleta, a avaliação e o processamento de informações (Knight, 2024) como ferramenta de tomada de decisão, a fim de identificar, alertar e prevenir riscos e ameaças, reduzindo a incerteza (Francisco & Barrilao, 2019). Para tal, estas tarefas

devem ser realizadas de forma intencional, atempada, planeada, "secreta" e organizada (Andric & Terzic, 2023).

2.1. TIPOS DE INTELIGÊNCIA

Existem várias classificações de inteligência, mas uma das mais comuns é de acordo com o meio em que a informação é encontrada, estabelecendo os seguintes tipos (Kamiński, 2019):

- **SIGINT** (*Signal Intelligence*): é derivada da intercepção de sinais, independentemente da forma como são transmitidos. Existem três subcategorias: inteligência de comunicações (COMINT), inteligência eletrónica (ELINT) e inteligência de sinais de instrumentação estrangeira (FISINT). É particularmente importante no controlo das ameaças digitais e dos conflitos híbridos.
- **MASINT** (*Measurement and Signature Intelligence*): baseia-se na medição de atributos físicos, como as emissões electromagnéticas, as propriedades químicas ou as características acústicas. É utilizada em operações militares avançadas e na deteção de armas com o objetivo de caracterizar, localizar e identificar alvos.
- **HUMINT** (*Human Intelligence*): é o método mais antigo de recolha de informações a partir de fontes humanas, seja através de entrevistas, observação direta, infiltração ou colaboração com actores locais. É essencial em contextos em que as tecnologias não podem aceder-lhe.
- **GEOINT** (*Geospatial Intelligence*) e **IMINT** (*Imagery Intelligence*): inteligência geoespacial e imagética. A primeira combina mapas, dados geográficos e informações de teledeteção, enquanto a segunda se centra na análise visual de imagens de satélite, aéreas ou de drones.
- **OSINT** (*Open-Source Intelligence*): inteligência derivada de informações do domínio público em formato físico, analógico ou digital em diferentes suportes, como a rádio, a televisão, os jornais, as revistas, a Internet, as bases de dados comerciais, os vídeos, os gráficos, os desenhos, as redes sociais, etc. relatórios abertos ou públicos. O seu volume, acessibilidade e utilidade aumentaram exponencialmente com a Internet (Stewart Bertram, 2015).
- **SOCMINT** (*Social Media Intelligence*): por vezes também referida como uma subcategoria da OSINT, centrada nos media sociais. É utilizada para monitorizar tendências, detetar ameaças emergentes, analisar perceções e seguir atores específicos (Mahood, 2015).

No entanto, outra tipificação comum é de acordo com a sua finalidade: estratégica, tática e operacional (Gruszczak, 2018).

- **Informação estratégica:** centra-se na identificação de riscos, ameaças e oportunidades para apoiar a definição de objectivos e a tomada de decisões, tendo em conta o ambiente, os intervenientes relevantes e as possíveis evoluções.
- **Informações táticas:** centram-se no planeamento e na execução de operações específicas para atingir um objetivo de âmbito limitado, derivado dos objectivos gerais das informações estratégicas.
- **Inteligência operacional:** também conhecida como inteligência operacional no âmbito militar, tem como objetivo permitir a organização e a execução de actividades para cumprir uma missão específica (Jiménez Villalonga, 2018).

A coexistência e a complementaridade entre estas categorias permitem construir uma inteligência global, adaptada aos diferentes níveis de decisão.

2.2. EVOLUÇÃO DAS ABORDAGENS E ESTRATÉGIAS DE INFORMAÇÃO

Muitos autores defendem que a inteligência é tão antiga quanto a história da humanidade, uma vez que esconder informações confidenciais e descobrir as dos adversários sempre foi uma ferramenta para alcançar e manter o poder. Assim o demonstram civilizações como a China antiga com a sabedoria milenar do mestre Sun Tzu (Navarro Bonilla, 2005) ou a Grécia clássica com os procedimentos secretos de transmissão de informação de Eneias, o Tático (Vela Tejada, 1993).

Na sua origem, a Intelligence era um instrumento ao serviço do poder político, com uma orientação eminentemente militar: conhecer a força, a localização e as capacidades do inimigo para facilitar a tomada de decisões do dirigente. No entanto, à medida que as sociedades se tornaram mais complexas, o mesmo aconteceu com as suas ameaças, o que levou à progressiva expansão da inteligência para aspectos sociais, económicos ou políticos. Assim, as actividades de Intelligence assumiram um papel crucial com o nascimento dos Estados e das relações entre eles, com o objetivo de defender e proteger os interesses nacionais (Andric & Terzic, 2023).

No entanto, só em meados do século XX, nomeadamente após as duas guerras mundiais e a Guerra Fria, é que as potências mundiais começaram a organizar formalmente os seus serviços de informações (os Estados Unidos com a CIA, o Reino Unido com o MI6 e Israel com a Mossad).

A Espanha, embora menos proeminente internacionalmente neste domínio, também fez a primeira tentativa de criar um serviço de informações por volta desta altura. Em 1972 foi criado o Serviço Central de Documentação (SECED) e em 1977 o Centro Superior de Informação de Defesa (CESID), mas só em 2002 foi fundado o atual CNI (Centro Nacional de Informações, 2023).

A partir de então, a revolução tecnológica e a explosão do volume de informação disponível marcaram uma mudança radical: a intelligence deixou de ser um domínio fechado e exclusivamente centrado no Estado para se tornar uma atividade transversal e dinâmica com implicações para além da esfera político-militar. Embora a essência das informações continue a ser a mesma, os métodos, o calendário e os objectivos sofreram profundas transformações. O acesso massivo a dados através de fontes abertas, a aceleração dos fluxos de informação e a globalização das ameaças reduziram o ciclo de vida da informação e puseram em causa o papel central anteriormente ocupado pelo secretismo (Payá-Santos, 2023).

A este novo contexto juntaram-se os atentados de 11 de setembro, que marcaram um ponto de viragem, evidenciando a necessidade de identificar e prevenir ameaças assimétricas e transnacionais, esbatendo a distinção clássica entre inteligência interna e externa, e empurrando as instituições policiais para a adoção de modelos mais analíticos, preventivos e colaborativos (Knight, 2024).

Com o progressivo alargamento da inteligência a outras áreas estratégicas, como o policiamento, que historicamente funcionava numa lógica reactiva, as funções policiais

começaram a evoluir significativamente. A sua abordagem clássica, centrada na resposta a crimes consumados ou na resposta a pedidos de serviço, foi posta em causa à medida que as mudanças sociais e a crescente complexidade da criminalidade exigiam novas formas de intervenção (Organização para a Segurança e Cooperação na Europa, 2017). Posteriormente, várias correntes filosóficas influenciaram o policiamento, tais como (Gkougkoudis et al., 2022):

- **Policiamento comunitário ou policiamento orientado para a comunidade (COP):** dá prioridade à cooperação entre os cidadãos e as agências de aplicação da lei, promovendo a confiança e a prevenção (Carter & Fox, 2019).
- **Policiamento para a resolução de problemas:** visa identificar e analisar os problemas subjacentes à criminalidade numa perspetiva mais ampla e transversal e procurar soluções estruturais e sustentáveis (Organização para a Segurança e Cooperação na Europa, 2017).
- **Policiamento de tolerância zero:** resposta rigorosa mesmo para delitos menores, baseada em ideias desenvolvidas por dois criminologistas americanos, James Q. Wilson e George Kelling, que em 1982 publicaram um artigo intitulado "Broken Windows" (Grabosky, 1999).

No entanto, nas últimas décadas, devido à complexidade das ameaças e dos riscos, muitos académicos e profissionais salientaram que a abordagem holística mais bem sucedida para combater a globalização da criminalidade é o *Intelligence-Led Policing* (ILP), que se traduz por policiamento baseado em informações. Esta abordagem surgiu na década de 1990 no Reino Unido como uma estratégia para melhorar a eficiência fiscal dos serviços policiais, ou seja, para otimizar a afetação de recursos, a produtividade operacional e a qualidade dos resultados do policiamento. Inicialmente implementada sobretudo para combater a criminalidade grave e organizada, evoluiu desde então a nível mundial como um modelo proactivo, impulsionado pela análise de dados e centrado na prevenção, redução e perturbação de todos os tipos de criminalidade. Nos Estados Unidos, foram os acontecimentos de 11 de setembro de 2001 que levaram finalmente à sua adoção, centrando a sua abordagem em formas mais complexas de criminalidade (Summers & Rossmo, 2019).

A ILP é uma filosofia proativa para identificar e prevenir problemas criminais usando dados brutos e análises mistas (quantitativas e qualitativas), mas não é uma tática pontual, mas uma estrutura flexível, adaptável e sustentável baseada em dados objetivos (Carter & Fox, 2019). No entanto, sua implementação enfrenta desafios em termos de clareza terminológica e integração de dados, bem como a necessidade de garantir o respeito aos direitos humanos na gestão da inteligência.

Paralelamente, o modelo de inteligência baseada em actividades (ABI) expandiu as capacidades analíticas, especialmente face a ameaças emergentes. Com antecedentes na Guerra Fria, o seu desenvolvimento foi impulsionado pela necessidade de gerir e analisar enormes volumes de dados gerados pelas tecnologias modernas, como os drones e as redes sociais, especialmente no contexto da luta contra o terrorismo. Os métodos tradicionais de análise revelaram-se inadequados neste novo ambiente, uma vez que os analistas passam demasiado tempo à procura de informações e a monitorizar alvos conhecidos, limitando a sua capacidade de descobrir o desconhecido. A ABI melhora este processo ao permitir a correlação em tempo real de dados provenientes de uma variedade

de fontes, ultrapassando as limitações dos métodos tradicionais de informação, vigilância e reconhecimento (ISR) (Atwood, 2015).

Outra abordagem relevante é o modelo 3i proposto por Ratcliffe em 2006, baseado em três pilares fundamentais: "interpretar", "influenciar" e "ter impacto" no ambiente criminal. Os analistas devem interpretar ativamente o ambiente, influenciar os decisores que, por sua vez, utilizam essa informação para conceber estratégias que afectam o ambiente criminal (Budhram, 2015). Em 2016, acrescentou mais um i, o da intenção, como se pode ver na Figura 1, destacando a necessidade de clareza e compreensão dos objectivos estabelecidos (Organização para a Segurança e Cooperação na Europa, 2017).

Figura 1
O modelo 4-i de Ratcliffe: intenção, interpretação, influência e impacto



Nota: Adaptado de *OSCE Guidance on Intelligence-led Policing* (p. 24), por OSCE, 2017, OSCE. *Intelligence-led Policing* (p. 24), pela OSCE, 2017, OSCE

Em suma, as informações evoluíram de uma atividade altamente secreta e centralizada para um processo transversal, interdisciplinar, distribuído e tecnologicamente apoiado. Esta evolução justifica a necessidade de novos modelos como o IDEM, que integram a análise humana com o processamento automatizado para fazer face às ameaças modernas, nomeadamente no ciberespaço. Além disso, esta trajetória permite-nos observar uma crescente convergência entre as lógicas de segurança, defesa e tecnologia, posicionando a inteligência como uma componente chave da soberania digital e da resiliência institucional.

3. O CICLO DA INTELIGÊNCIA

Embora Sherman Kent seja frequentemente creditado com a formulação científica do método de inteligência, pesquisas posteriores mostraram que uma metodologia rigorosa e um conjunto abrangente de operações (o que mais tarde ficou conhecido como o ciclo de inteligência) já foram delineados, por exemplo, durante a Guerra Civil Espanhola (Navarro Bonilla, 2004).

O ciclo de inteligência reúne todas as actividades que permitem a transformação da informação bruta em inteligência e, como o seu nome indica, tem um carácter cíclico. O ciclo de inteligência clássico tem quatro fases, mas em alguns países são acrescentadas

fases diferentes ou subfases diferenciadas. Por exemplo, em Espanha, o CCN-CERT estabelece seis fases para o ciclo de inteligência: direção e planeamento; recolha; transformação; análise e produção; disseminação e, finalmente, avaliação (Centro Criptológico Nacional, 2015).

- A primeira fase, designada por **direção e planeamento**, estabelece o quê e o como, ou seja, os requisitos do produto de informações a produzir e as acções a desenvolver para o obter. O objeto do estudo, o âmbito, os objectivos, o prazo e o tipo de relatório devem ser claros para que o trabalho nas restantes fases seja eficiente e resulte em maior qualidade e em conformidade com as normas legais nacionais e internacionais (Organização para a Segurança e Cooperação na Europa, 2017).
- Na fase seguinte, a **recolha**, são recolhidos dados brutos, por exemplo, das fontes acima mencionadas (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Este processo é complexo, uma vez que os analistas devem encontrar o equilíbrio certo entre a recolha de todos os dados necessários e suficientes sem cair numa sobrecarga de informação redundante. Para tal, devem estar conscientes da existência, relevância, acessibilidade e fiabilidade das fontes seleccionadas, bem como das restrições legais e dos requisitos de autorização (Organização para a Segurança e a Cooperação na Europa, 2017). Além disso, a validade e a exatidão das informações devem ser avaliadas antes de prosseguir com as restantes etapas do ciclo de informações.
- Na fase de **transformação**, os dados brutos recolhidos na fase anterior são convertidos em conjuntos estruturados, como bases de dados, referências bibliográficas, etc., transformando a informação nos formatos necessários para continuar o ciclo e obter inteligência. Esta fase consiste em catalogar, hierarquizar e referenciar a informação recolhida.
- A quarta fase, **análise e produção**, é composta pelas actividades através das quais a informação transformada é integrada, avaliada, analisada e preparada de modo a obter o produto final. Dentro desta fase, podem ser estabelecidas duas subfases: a primeira envolve a integração de dados obtidos de diferentes fontes para estabelecer hipóteses e identificar um padrão de inteligência; a segunda envolve a interpretação dos dados, ou seja, ir além das informações obtidas, refutando ou apoiando as hipóteses pré-estabelecidas (Organização para a Segurança e Cooperação na Europa, 2017). Geralmente, esta fase resulta naquilo a que se chama *inteligência acionável*, um produto de inteligência que responde aos requisitos definidos na fase de direção e planeamento e, portanto, às necessidades do consumidor. Este produto, por sua vez, pode ser de vários tipos, como uma análise de tendências, uma avaliação a longo prazo, uma informação atual, uma informação de estimativa ou de alerta, etc. (National Cryptologic Centre, 2015).
- Na fase de **divulgação**, o produto final é entregue ao consumidor que o solicitou e, se necessário e legalmente admissível, será também partilhado com outras partes interessadas.
- A última fase corresponde à **avaliação**, que permite o feedback contínuo de todas as fases anteriores do ciclo de inteligência com os resultados obtidos, permitindo o ajuste e o aperfeiçoamento das actividades individuais e do ciclo como um todo. Isto é particularmente útil para responder de forma otimizada às necessidades de informação em constante evolução.

No entanto, muitos especialistas põem em causa este modelo tradicional de inteligência e uma das críticas é a simplificação excessiva deste modelo em relação à grande complexidade do processo real de aquisição de inteligência. Robert Clark salienta que este termo "se tornou um conceito teológico: ninguém questiona a sua validade", apesar de não definir as etapas exactas a seguir (Phythian et al., 2013).

Além disso, Arthur Hulnick salienta que a noção de que os clientes dos serviços de informações orientam os produtores no início do ciclo é incorrecta, uma vez que os clientes esperam frequentemente ser alertados pelo sistema de informações, pelo que o processo de recolha é principalmente orientado pela necessidade de preencher lacunas de dados e não por orientações políticas (Pothoven et al., 2023).

Por outro lado, nem sempre os organismos de recolha de dados são abordados; muitas vezes, as bases de dados existentes que foram alimentadas durante anos são consultadas diretamente para preparar um relatório. Ou podem ser solicitados novos dados brutos às equipas que os recolhem, mas um novo pedido de informações não é normalmente feito ao nível do cliente (Jordán, 2011).

Quanto à fase de análise, a sua definição dentro do ciclo de inteligência não é criticada em si mesma, mas afirma-se que é a fase em que se cometem mais erros, não por falta de informação, mas pelo contrário, devido à sobrecarga de dados que leva a que a informação relevante seja ignorada ou interpretada de forma inadequada pelos analistas (Jordán, 2016). Os analistas precisam de estar conscientes dos seus próprios processos mentais e de potenciais erros, evitando simplificações cognitivas não intencionais e, claro, enviesamentos. Além disso, em alguns casos, como em situações de crise, os dados brutos chegam diretamente sem passar por esta fase.

No que se refere à fase de divulgação, esta também não é por vezes ultrapassada, uma vez que nem todas as análises produzidas chegam aos consumidores. Muitas não são lidas pelos destinatários e são armazenadas diretamente na base de dados interna. Noutros casos, é frequente os clientes já terem tomado as suas decisões e ignorarem as informações que não as apoiam.

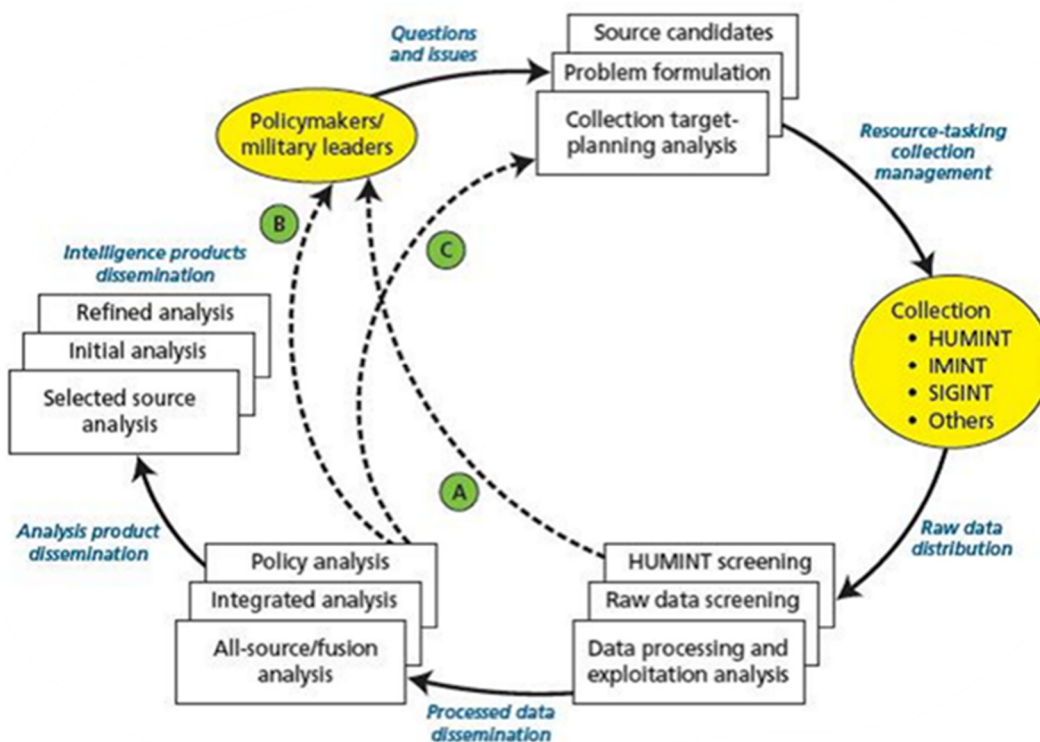
Além disso, em relação ao ciclo de inteligência em geral, critica-se a sua definição como uma sequência de fases que é finalmente organizada de forma circular, quando se trata de um processo mais dinâmico, onde todas as fases se retroalimentam, podendo avançar e retroceder em qualquer direção dentro do ciclo. Aponta também para problemas organizacionais, de comando e de fluxo de informação que conduzem a uma falta de flexibilidade na ação e na comunicação, atrasando os processos de tomada de decisão (Organização para a Segurança e Cooperação na Europa, 2017).

Comentadores como Peter Gill e Mark Phythian argumentam que o conceito de ciclo de informações se tornou obsoleto devido aos avanços tecnológicos, à revolução da informação e às mudanças nas ameaças e nos alvos. Propõem a sua substituição por uma "rede de informações" que reflecta melhor as interações complexas entre a definição de alvos, a recolha e a análise, e realça os factores contextuais que influenciam o processo e podem ser afectados pelos seus resultados (Pothoven et al., 2023).

Por outro lado, vários autores tentaram captar a complexidade do ciclo de inteligência em esquemas alternativos ao tradicional. Como se pode ver em Figura 2,

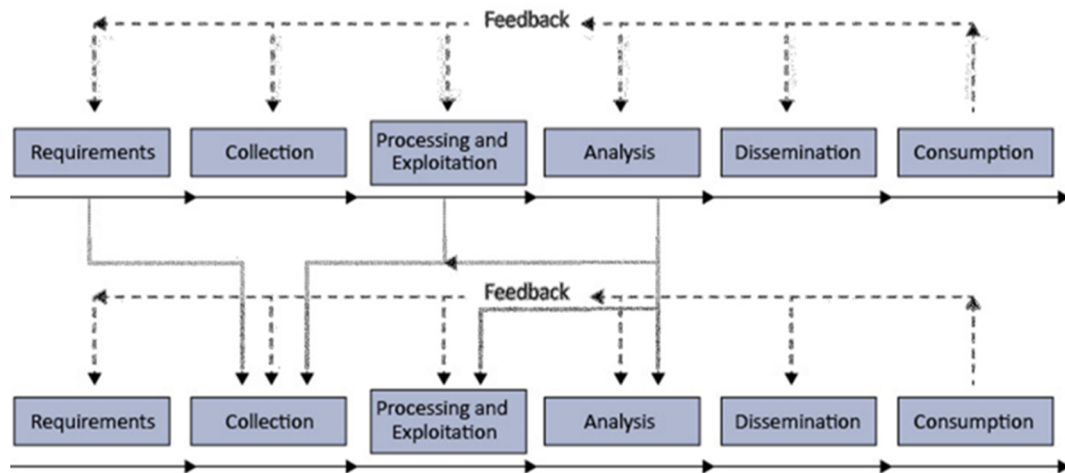
Treverton e Gabbard propõem uma abordagem mais realista que inclui atalhos entre fases, mostrando que há passos que por vezes são perdidos, por exemplo, que a informação não analisada pode chegar diretamente aos decisores. Mark Lowenthal apresenta um ciclo composto por feedbacks constantes, em que novas necessidades e ambiguidades reactivam o processo, tornando-o mais dinâmico e multifacetado, como se pode ver em Figura 3. E Robert M. Clark apresenta o conceito de *Target-Centric Intelligence*, um modelo colaborativo e orientado para o alvo, onde todos os participantes constroem juntos uma imagem partilhada da questão de inteligência de interesse, representada na Figura 4 (Jordan, 2016).

Figura 2
Abordagem de Treverton e Gabbard



Nota: Extraído de *A Review of the Intelligence Cycle* (p. 4) de J. Jordán, 2016, *Análise GESI* (Grupo de Estudos em Segurança Internacional), 2.

Figura3
 Processo multi-estratos Mark Lowenthal



Nota: Extraído de *A Review of the Intelligence Cycle* (p. 5) de J. Jordán, 2016, *Análise GESI (Grupo de Estudos em Segurança Internacional)*, 2.

Figura 4
 Inteligência centrada no alvo por Robert M. Clark



Nota: Extraído de *A Review of the Intelligence Cycle* (p. 6) de J. Jordán, 2016, *Análise GESI (Grupo de Estudos em Segurança Internacional)*, 2.

Por último, surgiram também propostas como o conceito JISR (Joint Intelligence, Surveillance and Reconnaissance) da NATO. Este termo refere-se ao conjunto integrado de capacidades de informações e operações que sincroniza e integra o planeamento e a execução de todas as capacidades de recolha de informações com o seu processamento, exploração e divulgação. Este conceito surge da necessidade de melhorar a partilha de informações e de informações para prevenir crises, ameaças terroristas, actividades criminosas transnacionais e ciberameaças (Gruszczak, 2018). A inteligência, a vigilância

e o reconhecimento (ISR) sempre foram actividades essenciais das operações militares, mas foram divididas de acordo com os níveis de comando (estratégico, operacional e tático), ou de acordo com as várias disciplinas de inteligência, dependendo do tipo e complexidade das fontes de informação envolvidas. No contexto atual, esta divisão limita a utilização óptima dos especialistas, agências, fontes e actividades de informações. Por conseguinte, é proposto o modelo JISR, em que as actividades de informações, vigilância e reconhecimento funcionam como uma unidade única, integrando todos os níveis e domínios (Ministério da Defesa, 2023).

No entanto, o modelo JISR apresenta o mesmo processo que o ISR, que é composto por 5 fases: planeamento, recolha, processamento, exploração e disseminação (TCPED). A principal diferença em relação ao ciclo tradicional de intelligence é que este processo não é linear nem circular, mas as diferentes fases são executadas de forma dinâmica, sequencial, simultânea ou independente, consoante o resultado pretendido. No entanto, neste modelo, o processo ISR está normalmente alinhado com a fase de recolha do ciclo de informações, e os resultados desta recolha são incorporados na fase de processamento, bem como apoiam o ciclo de decisão.

No entanto, esta abordagem também enfrenta várias limitações. Em primeiro lugar, pode haver uma falta de recursos suficientes para satisfazer todos os requisitos, especialmente devido à elevada procura e à baixa disponibilidade de certas capacidades de recolha. Há também problemas técnicos, como limitações na capacidade de computação e na largura de banda, que afectam a capacidade de processar e divulgar resultados. Os adversários podem interferir através de ataques às capacidades ISR, camuflagem, ocultação e desinformação. Além disso, o acesso à ISR pode ser limitado por barreiras físicas, cognitivas, virtuais, jurídicas e políticas (Ministério da Defesa, 2023).

A inteligência como processo atual deve, portanto, afastar-se dos modelos tradicionais lineares e cíclicos para estruturas mais fluidas e em rede, capazes de responder com agilidade às ameaças emergentes e tirar partido do vasto volume de dados disponíveis (Jiménez Villalonga, 2018).

4. PROPOSTA DE ACTUALIZAÇÃO DO CICLO DE INTELIGÊNCIA NA ERA DIGITAL: O MODELO IDEM

O ciclo clássico dos serviços de informações foi durante décadas a espinha dorsal dos serviços de informações enquanto processo. Na altura, esta representação sequencial fazia sentido, pois facilitava a normalização, a formação dos analistas e a gestão das operações. No entanto, o modelo tem limitações significativas quando transposto para os actuais contextos de complexidade, incerteza e ritmo acelerado de mudança, especialmente em domínios como o ciberespaço.

Neste ambiente altamente dinâmico, a inteligência tornou-se extremamente importante como ferramenta para compreender e antecipar ameaças, particularmente no domínio digital. À medida que as organizações expandem a sua presença no ciberespaço para maximizar a sua visibilidade e alcance, também aumentam a sua exposição a potenciais ataques. Esta transformação exige que se repense o papel da inteligência para além da sua formulação clássica, adaptando-a às particularidades de um ambiente descentralizado, interligado e em constante evolução.

No entanto, esta adaptação não é simples. A proliferação de termos e abordagens reflecte tanto a juventude do campo como a sua rápida expansão. Em alguns quadros conceptuais, o termo ciberinteligência ou CYBINT é utilizado como um subtipo de COMINT (Jiménez Villalonga, 2018), mas também pode ser considerado como um tipo de inteligência superior que engloba e coordena as actividades OSINT, SIGMINT, SOCMINT e até HUMINT (Portillo, 2019).

No contexto europeu, é mais comum falar-se de inteligência contra ciberameaças (CTI), que se refere à aplicação sistemática da inteligência para identificar, analisar e mitigar as ameaças que afectam o ciberespaço. Segundo a Gartner (Lee, 2023), a CTI assenta em conhecimentos baseados em provas que fornecem contexto, mecanismos, indicadores e conselhos práticos sobre ameaças emergentes ou existentes.

É por isso que a CTI desempenha um papel crucial ao ajudar as organizações a desenvolver uma estratégia de segurança proactiva que lhes permite compreender e antecipar as tácticas, técnicas e procedimentos (TTP) dos adversários. Também facilita a identificação de ameaças na sua origem e a resposta efectiva a incidentes antes que estes possam causar danos significativos.

No entanto, quando se trata de implementar sistemas de investigação ou de trabalho neste domínio, continua a não haver ciclos metodológicos específicos e amplamente aceites para estruturar o processo de recolha e análise de ciberinteligência. Por conseguinte, existe uma tendência para recorrer ao ciclo tradicional de recolha de informações ou a uma das abordagens alternativas existentes. Mas, como já foi referido, todas elas apresentam limitações significativas para a sua aplicação efectiva em ambientes digitais.

O modelo clássico é rígido e sequencial; o **modelo proposto por Treverton e Gabbard** permite alguma flexibilidade, mas carece de um feedback claro; o **modelo centrado no objetivo** propõe um ciclo contínuo mais próximo do objetivo, mas sem uma estrutura verdadeiramente flexível entre fases; e a **abordagem multinível de Lowenthal** introduz dinamismo, mas mantém uma certa linearidade e as ligações bidireccionais entre fases não são totalmente compreendidas.

Tabela 1

Quadro comparativo dos diferentes modelos de representação da inteligência como processo

	Modelo clássico	Modelo Treverton e Gabbard	Modelo por Mark Lowenthal	Modelo centrado no alvo
Estrutura	Linear ou cíclico (fases sucessivas num círculo)	Semi-linear (com possíveis "atalhos")	Multinível (com camadas activas conforme necessário)	Cíclico (centrado no objetivo)
Início do processo	A pedido do consumidor	Semelhante ao clássico, mas permite reiniciar a partir de fases intermédias.	De novas necessidades para reativar fases anteriores	Da análise do objetivo (de análises anteriores ou de novas necessidades e informações)
Fases principais	Direção e planificação, recolha, tratamento, análise e produção, difusão, avaliação	Semelhante ao modelo clássico, mas sem ordem estrita ou menção de feedback.	O mesmo que o clássico, com ciclos internos e <i>feedback</i> contínuo.	Os requisitos e <i>as lacunas</i> , a recolha, a análise e a divulgação estão interligados em torno do objetivo de
Interação entre fases	Limitado (feedback no final)	Médio (linear com atalhos)	Descarga (contínua e simultânea)	Média (ciclos ligados pelo objetivo)
Flexibilidade e adaptabilidade	Baixo (modelo rígido e sequencial)	Médio (alguma fluidez, mas mantém fases definidas)	Elevada (orientada para a reformulação contínua do processo)	Médio: (dinamismo em torno do objetivo)
Divulgação de informações	No final do processo	Pode ser omitido ou antecipado se o produto o exigir.	Pode ocorrer em diferentes níveis e momentos, dependendo do ciclo interno ativado.	Fim do processo, após a fase de produção
Feedback	No final do processo	Não explicitamente referenciado	Em todas as fases	Não explicitamente referenciado

É por isso que este trabalho propõe o modelo de inteligência IDEM (Enhanced Dynamic Enriched Intelligence) com uma abordagem em rede, não linear e altamente adaptativa, em que as fases do processo de inteligência não se seguem sequencialmente, mas interagem de forma dinâmica, flexível e contínua, permitindo um feedback constante entre fases e equipas de trabalho.

Enquanto o modelo tradicional começa com a **direção e o planeamento**, onde os requisitos de informação são estabelecidos de acordo com as necessidades do decisor, o modelo IDEM propõe começar com uma fase de **identificação e priorização das ameaças** em tempo real. Uma das críticas mais repetidas ao ciclo tradicional é a sua falta de flexibilidade, pois uma vez definidos os objectivos, o processo tende a seguir uma trajetória fixa, o que é ineficaz no contexto atual, em que as ameaças evoluem rapidamente e nem sempre estão alinhadas com as necessidades previamente estabelecidas. Por conseguinte, o objetivo desta fase deve ser detetar e dar prioridade às ameaças emergentes de forma proactiva, sem depender apenas das orientações iniciais dos consumidores, que muitas vezes não chegam a tempo ou nem sequer são formuladas.

Esta fase tornar-se-ia um processo dinâmico e contínuo, alimentado por uma monitorização constante, pelo reconhecimento em tempo real de padrões de ameaças emergentes e pela capacidade de redirecionar rapidamente os esforços de informação à medida que surgem novas ameaças ou mudanças nas condições (Dahj, 2022).

A fase seguinte, a **recolha**, continua a ser fundamental para os serviços de informações enquanto processo, uma vez que sem dados e informações não é possível obter conhecimentos acionáveis. No modelo clássico, um dos maiores desafios tem sido o de filtrar eficazmente grandes volumes de dados para evitar tanto a saturação da informação como a perda de informação crítica. Na Era Digital, esta tarefa tornou-se ainda mais complexa devido ao aumento exponencial da quantidade de fontes e dados disponíveis, impulsionado pelas novas tecnologias, pela globalização e pelo curto prazo de validade da informação. A IDEM aborda esta complexidade através da utilização de tecnologias avançadas, como a *aprendizagem automática* (ML) e a inteligência artificial, que permitem uma recolha automatizada, contínua e abrangente. Apesar de tratarem volumes significativamente maiores, estas ferramentas permitem filtrar, hierarquizar e enriquecer a informação em tempo real, garantindo a sua relevância e utilidade.

Nesta abordagem, não faz sentido estabelecer uma fase específica para a **transformação** de dados, como no modelo clássico. Graças a tecnologias avançadas, como o processamento de linguagem natural (PNL) e as ferramentas de análise *de grandes volumes de dados*, a conversão de dados brutos em informações relevantes e contextualizadas pode ocorrer em várias fases do processo em simultâneo. Isto permite que os dados sejam processados, estruturados e analisados em paralelo, facilitando uma resposta ágil a novas informações ou alterações no ambiente.

Além disso, a separação entre **transformação** e **análise** pode levar a uma falta de integração e a uma perda de contexto durante a transição. Por esta razão, o IDEM substitui estas duas fases do modelo clássico por uma única fase de **contextualização e enriquecimento** que se concentra em colocar os dados no contexto, interpretar a sua relevância e compreender a ligação a outros eventos e padrões. Desta forma, a análise pode ser continuamente actualizada e ajustada à medida que surgem novos dados e novas questões, desenvolvendo uma capacidade de adaptação contínua. É também essencial processar e integrar informações de múltiplas fontes de dados, uma vez que estas facilitam uma interpretação mais profunda e eficiente, especialmente no atual contexto de ameaças híbridas. Ao contrário da abordagem tradicional, e também dos sistemas ISR clássicos, que estabelece um processo individual para cada tipo de fonte (OSINT, HUMINT, SIGINT, COMINT, etc.) (Ministério da Defesa, 2023), a IDEM propõe um modelo interconectado, multi-sensor, mais eficaz na deteção e análise de fenómenos complexos, tal como sugerido pela doutrina JISR do Departamento de Defesa dos EUA, discutida na secção 2.2

Em contrapartida, o modelo IDEM mantém uma etapa específica para a **produção de** inteligência acionável. Enquanto, no ciclo tradicional, a análise e a produção se concentram na geração de relatórios e recomendações que auxiliam a tomada de decisão, o IDEM defende produtos não apenas reativos, mas também preditivos, permitindo a antecipação de eventos e tendências ou a avaliação de impactos que facilitem o ajuste de estratégias e decisões em tempo real. A tónica é colocada aqui na inteligência como apoio dinâmico à decisão e não como um produto fechado.

Paralelamente ao desenvolvimento de todas estas fases, a fase de **feedback** definida no ciclo de inteligência tradicional é indispensável, mas reinterpretada como um processo transversal. Para garantir uma melhoria contínua e um processo mais eficaz, é fundamental que os pontos de melhoria ou os pontos fracos sejam evidenciados ao longo de cada uma das fases. Isto permitirá que estas observações sejam tidas em conta não só nas etapas seguintes, mas também em futuras investigações, em vez de se esperar pela obtenção do produto final de intelligence, como acontece no modelo tradicional.

Finalmente, no ciclo tradicional, a **disseminação** é reservada para o final do processo, uma vez produzido o relatório de intelligence. O IDEM rompe com esta lógica, propondo uma divulgação modular e progressiva, não só partilhando a inteligência enquanto tal, mas também as ameaças reconhecidas e classificadas na fase de identificação e priorização, ou os dados recolhidos das diferentes fontes disponíveis ou ainda os dados contextualizados e enriquecidos em diferentes formatos. Obviamente, esta difusão precoce deve ser cuidadosamente gerida, assegurando a proteção das fontes para evitar contramedidas e desinformação por parte dos alvos e para proteger as fontes humanas (HUMINT). No entanto, a natureza transnacional dos crimes actuais exige a cooperação internacional de diferentes serviços de informações e, por conseguinte, a partilha atempada e não retardada de informações entre eles para obter resultados mais eficazes.

No entanto, apesar das capacidades técnicas oferecidas pela automatização, o papel do analista humano continua a ser essencial em cada uma das fases acima descritas. As ferramentas automatizadas funcionam com parâmetros e algoritmos definidos pelos seus programadores, que são verdadeiramente capazes de interpretar a informação num contexto mais amplo, tendo em conta factores culturais, políticos e situacionais. Além disso, os modelos preditivos não têm a flexibilidade cognitiva necessária para lidar com ambiguidades, contradições ou excepções e podem falhar face a entradas erradas, dados tendenciosos ou situações imprevistas.

Os analistas, por outro lado, são capazes de se adaptar, inovar e reajustar as suas abordagens em resposta a novos paradigmas, enquanto os modelos de inteligência artificial necessitam de uma grande quantidade de dados de treino para poderem desenvolver novas metodologias de análise e não são capazes de aplicar abordagens criativas se surgirem novas questões. Esta capacidade dos humanos de colaborar entre equipas, de discutir interpretações, de reestruturar estratégias com base no *feedback* recebido é essencial para o sucesso da implementação de estratégias de inteligência (Jordan, 2011).

Tabela 2
Quadro comparativo entre o modelo clássico e o modelo IDEM proposto

	Modelo clássico	Modelo IDEM (proposta própria)
Estrutura	Linear ou cíclico (fases sucessivas num círculo)	Modular, dinâmico e em rede (círculos concêntricos e interligados)
Início do processo	A pedido do consumidor	Proactivo, sem pedido prévio
Fases principais	Direção e planificação, recolha, tratamento, análise e produção, difusão, avaliação	Identificação e definição de prioridades, recolha, contextualização e enriquecimento, produção de informações, feedback e divulgação
Interação entre fases	Limitado (feedback no final)	Descarga: fases interactiva e bidireccional
Flexibilidade e adaptabilidade	Baixo (modelo rígido e sequencial)	Muito elevado (fases simultâneas e reiniciáveis)
Divulgação de informações	No final do processo	Transversal e contínuo desde as fases iniciais do processo
Feedback	No final do processo	Constante: em todas as fases
Tecnologia aplicada	Não explicitamente abrangido	Integração de tecnologias avançadas (IA, ML, PNL, <i>grandes volumes de dados</i>)
Participação humana	Central, mas hierárquico	Combinação sinérgica de analistas humanos e ferramentas automatizadas
Aplicabilidade em ambientes digitais	Limitada	Elevada (orientada para as ciberameaças e cenários complexos)

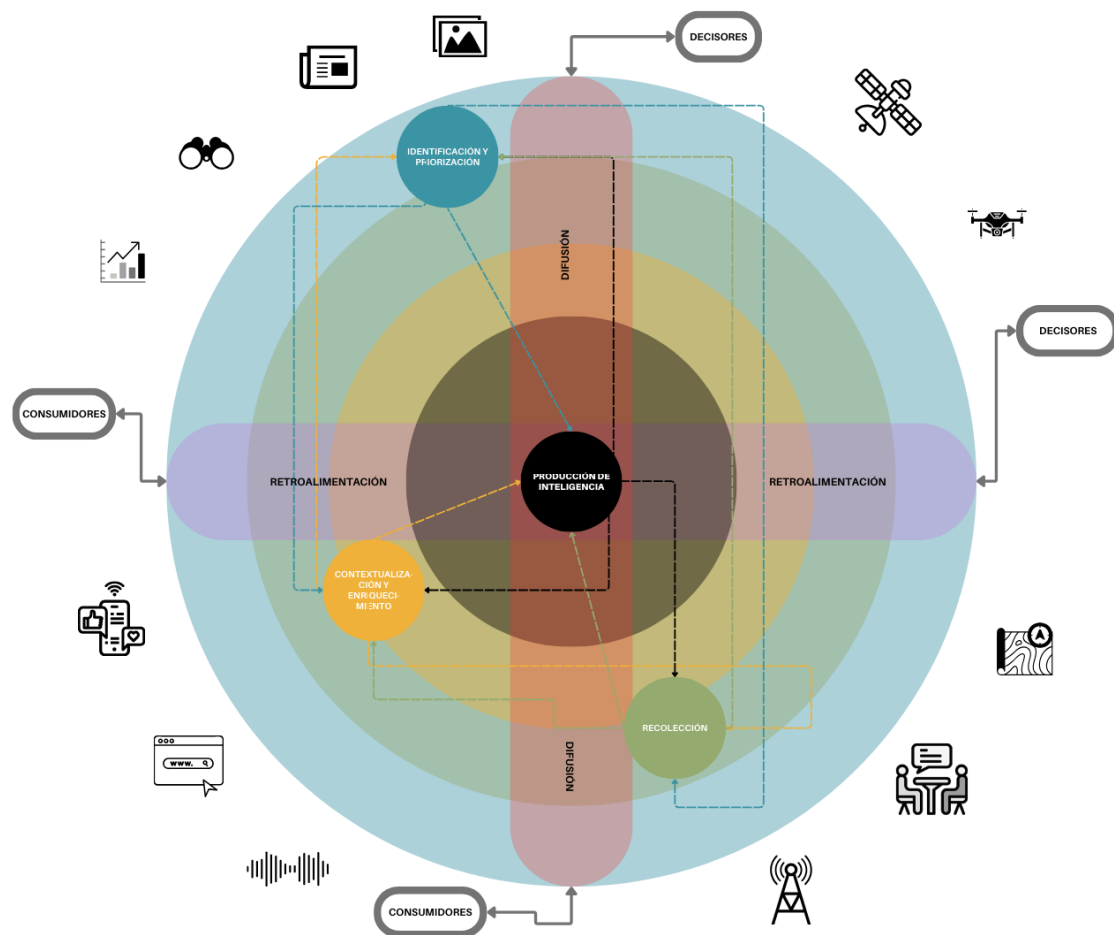
A seguir é apresentado um esquema representativo do modelo IDEM, no qual as diferentes fases estão dispostas em círculos concêntricos. Esta disposição reflecte, por um lado, a proximidade crescente do produto final da inteligência à medida que nos aproximamos do centro e, por outro lado, a natureza constante de todas as fases, uma vez que as fases mais internas estão contidas nas mais externas. No entanto, o modelo não estabelece um percurso linear, não é necessário passar por todas as fases para chegar ao centro. Este carácter dinâmico é representado por setas que indicam os possíveis fluxos de entrada e saída entre as diferentes fases, permitindo transições diretas e bidireccionais de acordo com as necessidades do contexto.

Perpendicularmente a estes círculos e perpendicularmente entre si, integram-se dois elementos-chave, representados como rectângulos transversais. O primeiro representa a fase de feedback, transversal a todas as fases e oportuna para a melhoria contínua de todo o ciclo. O segundo simboliza a fase de disseminação, também colateral a todas as fases e essencial para obter produtos mais completos e resultados mais eficazes.

No exterior do sistema encontram-se os consumidores e os decisores. O seu número e relevância dependerão tanto das necessidades de informação requeridas como do impacto esperado da análise efectuada. Estas figuras são representadas por setas bidireccionais, que indicam a sua dupla função de estabelecer o objetivo e os critérios das informações, ao mesmo tempo que recebem feedback ou produtos de informações para facilitar a sua tomada de decisão.

São também incorporados ícones de diferentes fontes de informação, apoiando assim a estratégia de recolha, contextualização e enriquecimento de dados de diferentes fontes para um processo de informação mais abrangente, transversal e eficaz.

Figura 5
Modelo de inteligência IDEM



Nota: Elaboração própria, Paula Castro Castañer, 2024.

A combinação da adaptabilidade, da experiência, do juízo crítico e do talento humano com a capacidade das máquinas para processar grandes volumes de dados cria uma sinergia que garante uma tomada de decisões mais eficaz, multidisciplinar, informada e flexível, assegurando uma maior qualidade e relevância da inteligência gerada.

4.1. EXEMPLO PRÁTICO DA APLICAÇÃO DO MODELO IDEM

Um exemplo prático que ilustra a utilidade da aplicação deste modelo de inteligência é o caso de um fornecedor nacional de energia detetar uma anomalia nos seus sistemas de controlo SCADA. Nesta situação, não existe ainda um incidente confirmado ou um pedido explícito dos decisores (uma vez que estes provavelmente ainda não têm conhecimento desta situação), o que implica que a ativação do processo de inteligência tenha origem de forma proactiva e autónoma, com base em sinais identificados no

ambiente operacional. No entanto, a equipa de informações internas ativa o modelo IDEM para antecipar se se trata de uma ameaça real ou de um falso alarme.

Um alerta automático de tráfego anómalo para os servidores de backup provém do IDS, que inicia a fase de identificação e priorização. Este alerta, embora preliminar, é suficiente para que a equipa de inteligência interna classifique a ameaça como prioritária, tendo em conta o potencial impacto que um compromisso desta natureza pode ter nas infra-estruturas críticas do país. Em consequência, decide-se despriorizar temporariamente as investigações abertas sobre campanhas hacktivistas e a vigilância geopolítica de baixo impacto, bem como outras tarefas de monitorização de rotina em fóruns e canais obscuros. Esta reorientação permite concentrar os esforços humanos e tecnológicos numa única hipótese de trabalho: uma possível intrusão avançada direcionada.

A recolha é desencadeada simultaneamente a partir de múltiplas fontes internas (logs, SIEM, registos de autenticação) e externas (feeds de ciberinteligência, bases de dados de indicadores de comprometimento, alertas de entidades cooperantes ou fornecedores de informações). Durante esta fase, quando surgem indícios que sugerem motivações económicas por detrás do possível ataque, como, por exemplo, a extração de dados de mercado em vez de informação operacional, o processo regressa brevemente à fase de identificação para reformular a hipótese inicial. Este regresso permite que a análise se centre agora na possibilidade de um caso de espionagem económica industrial em desenvolvimento, mudando consequentemente o foco do resto das actividades do processo de informações.

Na fase de contextualização e enriquecimento, os dados recolhidos são integrados com informações históricas de incidentes anteriores e análises de tendências no sector da energia. São utilizadas técnicas de análise comportamental, de atribuição de TTP e de extração de dados históricos. Estas metodologias facilitam a deteção de padrões e coincidências com campanhas previamente atribuídas a actores estatais ou a grupos intermediários, ou seja, entidades que operam como proxies ou agentes indirectos de outros actores com interesses geopolíticos ou económicos.

Os resultados das informações são distribuídos em diferentes formatos, adaptados às necessidades específicas de cada tipo de destinatário. Entre eles contam-se os alertas táticos dirigidos às equipas de cibersegurança responsáveis pela resposta imediata, os relatórios estratégicos dirigidos aos gestores de topo dos sistemas de energia e as recomendações preventivas dirigidas a outros operadores do sector para que reforcem a sua postura de defesa.

É importante notar que esta produção e divulgação de informações é feita de forma contínua e em paralelo com o desenvolvimento da investigação, sem esperar por uma "conclusão definitiva". Esta abordagem permite uma resposta precoce e dinâmica a ameaças emergentes, uma vez que outros actores relevantes no sector da energia poderiam reportar incidentes semelhantes nas suas redes após a receção destes produtos, o que permitiria reabrir ciclos de análise e reajustar a priorização de ameaças à escala nacional.

Para além do feedback externo dos intervenientes relevantes para ajustar os pressupostos e as prioridades com base nos sinais do ambiente, há também uma fase de feedback interno contínuo destinada a melhorar o próprio processo de informações. Por

exemplo, durante a fase de contextualização, a equipa de informações detecta que certos indicadores-chave de comprometimento (IoCs) não foram inicialmente priorizados pelos sistemas de alerta automatizados. Esta observação é documentada e canalizada para a equipa responsável pelo ajuste dos limiares de sensibilidade do SIEM, o que permite aperfeiçoar os critérios de deteção para futuros casos semelhantes. Finalmente, no final do ciclo, é efectuada uma revisão interna do desempenho do modelo IDEM neste caso específico, avaliando métricas como o tempo de resposta, a precisão das hipóteses iniciais e a utilidade dos produtos gerados. Esta avaliação alimenta uma base de conhecimento interna que permite o ajuste de metodologias, ferramentas e fluxos de trabalho, garantindo que o modelo evolui de forma adaptativa e com base na experiência acumulada.

Esta dinâmica de retrocesso, reformulação e ação simultânea permitida pelo modelo IDEM seria impraticável no modelo clássico do ciclo de inteligência, nem em muitos dos modelos propostos na literatura revista, onde os processos são mais rígidos, lineares e dependentes da iniciativa dos decisores.

5. CONCLUSÕES

A inteligência, entendida como organização, processo, produto e mesmo cultura, desempenha um papel fundamental na gestão da incerteza em ambientes de ameaça voláteis, interligados e cada vez mais híbridos. A sua natureza multidisciplinar e a diversidade de abordagens utilizadas por diferentes países e disciplinas dificultam uma definição única e uma classificação fechada dos seus tipos, mas reflectem também a sua riqueza concetual e a necessidade de cooperação e adaptação constante.

O ciclo clássico da informação, embora valioso na altura por fornecer estrutura e normalização, tem limitações significativas para responder aos desafios contemporâneos, especialmente no domínio digital. A natureza dinâmica e descentralizada do ciberespaço, bem como o volume e a velocidade dos dados, exigem modelos mais flexíveis e adaptáveis. O modelo IDEM proposto neste documento responde a esta necessidade através de uma estrutura modular, não linear e em rede, em que as fases interagem simultaneamente e se retroalimentam constantemente umas às outras.

Esta nova abordagem reorganiza as fases do ciclo tradicional e acrescenta elementos-chave como a identificação proactiva de ameaças, a contextualização integrada com a análise, a divulgação precoce e transversal de informações e a incorporação sistemática de feedback. Integra também tecnologias avançadas, como a inteligência artificial e a aprendizagem automática, para otimizar a gestão de grandes volumes de dados e melhorar as capacidades de previsão.

No entanto, a tecnologia, por si só, não é suficiente. O discernimento humano, a capacidade crítica, a criatividade analítica e o conhecimento contextual continuam a ser essenciais. A sinergia entre os analistas e os sistemas automatizados garante uma informação mais eficiente, exacta e útil para a tomada de decisões.

Em suma, a inteligência do século XXI deve ser ágil, multidisciplinar e colaborativa. Só através de abordagens híbridas, abertas à aprendizagem e à melhoria contínua, será possível antecipar e mitigar eficazmente as ameaças emergentes. O modelo IDEM é um passo nessa direção: uma proposta adaptativa e realista para responder aos desafios que a era digital impõe aos sistemas de intelligence contemporâneos.

A realidade do contexto atual continua a apresentar desafios e dificuldades significativas para antecipar e mitigar eficazmente as ameaças contemporâneas, sobretudo as que se manifestam no ciberespaço, pois é difícil acompanhar e antecipar-se aos cibercriminosos. É, pois, necessário que a comunidade de informações continue a investigar e a desenvolver estratégias que diminuam as actuais fragilidades, promovam a sensibilização para a cultura de informações, a divulgação de informações e a cooperação internacional.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- Andric, J., & Terzic, M. (2023). Ciclo de inteligência na luta contra o terrorismo com o uso de dados OSINT. *Jornal de Sistemas de Informação e Gestão de Operações*, 17(1). <https://doi.org/10.1080/2158379X.2021.1879572>
- Atwood, C. P. (2015). Inteligência baseada em atividades revolucionando a análise de inteligência militar. *Joint Force Quarterly*, 77. <https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/>
- Budhram, T. (2015). Policiamento baseado em informações: uma abordagem proactiva para combater a corrupção. *South African Crime Quarterly*, 52. <https://doi.org/10.17159/2413-3108/2015/i52a30>
- Carter, J. G., & Fox, B. (2019). Policiamento comunitário e policiamento liderado por inteligência: um exame da validade convergente ou discriminante. *Policing: An International Journal*, 42(1), 43-58. <https://doi.org/10.1108/PIJPSM-07-2018-0105>
- Centro Nacional de Criptologia (2015). CCN-STIC-425 Ciclo de Inteligência e Análise de Intrusão.
- Centro Nacional de Informações (2023). Origens dos Serviços de Informações. <https://www.cni.es/sobre-el-cni/nuestra-historia>
- Chainey, S., & Chapman, J. (2013). Uma abordagem orientada para o problema para a produção de avaliações de inteligência estratégica. *Policing: An International Journal of Police Strategies & Management*, 36(3), 474-490. <https://doi.org/10.1108/PIJPSM-02-2012-0012>
- Dahj, J. N. M. (2022). Dominando a inteligência cibernética. Packt Publishing Ltd.
- Díaz Fernández, A. M. (2013). O papel da inteligência estratégica no mundo atual. *Cuadernos de Estrategia*, 162, 35-66. <https://dialnet.unirioja.es/servlet/articulo?codigo=4275959>
- Francisco, J., & Barrilao, S. (2019). Serviços de inteligência, sigilo e garantia judicial de direitos. *Teoría y Realidad Constitucional*, 309-340.

- Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. *Digital*, 2, 143-163. <https://doi.org/10.3390/digital2020009>
- Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).
- Gruszczak, A. (2018). O desafio da adaptação das informações da NATO. <https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge>
- Jefatura del Estado (2002). Lei 11/2002, de 6 de maio, que regula o Centro Nacional de Informações.
- Jiménez Villalonga, R. (2018, 26 de novembro). Tipos de inteligência. <https://global-strategy.org/tipos-de-inteligencia/>
- Jordán, J. (2011). Introdução à análise de inteligência. 2340-8421, 2, Art. 2. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Jordán, J. (2016). Uma revisão do Ciclo de Inteligência. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Kamiński, M. A. (2019). Fontes de Inteligência no Processo de Coleta de Informações pela Comunidade de Inteligência dos EUA. *Security Dimensions*, 32(32), 82-105. <https://doi.org/10.5604/01.3001.0014.0988>
- Knight, T. C. (2024). Five Thousand Candles: Optimizing Information Sharing Policies for Homeland Security Uma dissertação. Sistema Universitário Público Americano.
- Lee, M. (2023). *Cyber Threat Intelligence* (1ª ed.), John Wiley & Sons, Inc.
- Mahood, L. M. E. K. (2015). SOCMINT: seguindo e gostando de inteligência de mídia social [Canadian Forces College]. <https://www.cfc.forces.gc.ca/254-eng.html>
- Ministério da Defesa (2023). Informações, vigilância e reconhecimento.
- Montero Gómez, A. (2006). Inteligencia Prospetiva de Seguridad (24; Área: Segurança e Defesa). <https://www.realinstitutoelcano.org/publicaciones/>
- Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51-66. <https://dialnet.unirioja.es/servlet/articulo?codigo=2270935>

- Navarro Bonilla, D. (2005). Informação, espionagem e inteligência na monarquia hispânica (séculos XVI-XVII). *Revista de Historia Militar, Extraordinario*, 13-40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075
- Organização para a Segurança e a Cooperação na Europa (2017). Guia da OSCE sobre policiamento baseado em informações (Unidade de Assuntos de Polícia Estratégica do Departamento de Ameaças Transnacionais, Ed.; Vol. 13).
- Payá-Santos, C. A. (2023). O desempenho da inteligência em Espanha nos âmbitos público, empresarial e académico. *Revista Científica General José María Córdova*, 21(44), 1029-1047. <https://doi.org/10.21830/19006586.1222>
- Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). *Compreendendo o Ciclo da Inteligência* (M. Phythian, Ed.).
- Portillo, I. (2019). Saber o que é Cyber Intelligence e Cyber Threat Intelligence. <https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/>
- Pothoven, S., Rietjens, S., & de Werd, P. (2023). Paradigmas produtor-cliente para inteligência de defesa. *Estudos de Defesa*, 23(1), 68-85. <https://doi.org/10.1080/14702436.2022.2089658>
- Stewart Bertram (2015). *O Tao da Inteligência de Código Aberto*. IT Governance Publishing.
- Summers, L., & Rossmo, D. K. (2019). Entrevistas de infratores: implicações para o policiamento baseado em informações. *Policing*, 42(1), 31-42. <https://doi.org/10.1108/PIJPSM-07-2018-0096>
- Vela Tejada, J. (1993). Tradição e originalidade na obra de Eneias, o Tático: A génese da historiografia militar. *Minerva. Revista de Filología Clásica*, 7, 79-92. <https://doi.org/https://doi.org/10.24197/mrfc.7.1993>



Artigo de investigação

HACKTIVISMO: DO PROTESTO SOCIAL À INSTRUMENTALIZAÇÃO DO ESTADO

Tradução para o português com ajuda de IA (DeepL)

Josué Expósito Guisado
Sargento da Guardia Civil
Estudante de doutoramento na Universidade Pablo de Olavide
Mestrado em Paz, Segurança e Defesa pelo
Instituto Universitario Gutiérrez Mellado (UNED)
jexpgui@gmail.com
ORCID: 0009-0003-4977-3899

Recebido em 18/03/2025

Aceite em 05/05/2025

Publicado em 27/06/2025

Citação recomendada: Expósito, J. (2025). Hacktivismo: do protesto social à instrumentalização do Estado. *Revista Logos Guardia Civil*, 3(2), pp. 101-122.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

HACKTIVISMO: DO PROTESTO SOCIAL À INSTRUMENTALIZAÇÃO DO ESTADO

Resumo: INTRODUÇÃO. 2. DO PROTESTO SOCIAL À GUERRA CIBERNÉTICA. 3. 3.A LIGAÇÃO ENTRE HACKTIVISMO E APT. 4. O FUTURO DOS GRUPOS HACKTIVISTAS. 5. CONCLUSÕES. 6. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: O hacktivismo evoluiu de uma forma inicial de protesto digital para se tornar um instrumento fundamental nos conflitos geopolíticos contemporâneos. O que começou por ser um movimento descentralizado em defesa da liberdade de expressão e da justiça social tem sido progressivamente instrumentalizado pelos Estados para executar ciberataques, manipular a opinião pública e lançar operações de desinformação. Este fenómeno foi particularmente acentuado no contexto da guerra na Ucrânia, onde a convergência entre grupos de Ameaças Persistentes Avançadas (APT) e hacktivistas patrióticos permitiu a execução de ciberoperações coordenadas com os interesses do Estado. Paralelamente, a internacionalização do hacktivismo levou à formação de alianças entre grupos de diferentes regiões, alargando o seu impacto para além do conflito russo-ucraniano. O ciberespaço estabeleceu-se como uma arena ideal para o confronto entre Estados num ambiente controlado. No entanto, a crescente sofisticação dos ataques e o facto de visarem alvos cada vez mais estratégicos colocam sérios desafios à estabilidade internacional e à segurança dos Estados ocidentais.

Resumen: El hacktivismo ha evolucionado desde una forma inicial de protesta digital hasta convertirse en una herramienta clave en los conflictos geopolíticos contemporáneos. Lo que comenzó como un movimiento descentralizado en defensa de la libertad de expresión y la justicia social, ha sido progresivamente instrumentalizado por los Estados para ejecutar ciberataques, manipular la opinión pública y desplegar operaciones de desinformación. Un fenómeno que se ha visto especialmente acentuado en el marco de la guerra de Ucrania, donde la convergencia entre grupos de Amenaza Persistente Avanzada (APT) y hacktivistas patrióticos ha permitido la ejecución de operaciones cibernéticas coordinadas con los intereses estatales. Paralelamente, la internacionalización del hacktivismo ha llevado a la formación de alianzas entre grupos de distintas regiones, ampliando su impacto más allá del conflicto ruso-ucraniano. El ciberespacio se ha consolidado como un escenario idóneo para la confrontación entre Estados en un entorno controlado. Sin embargo, la creciente sofisticación de los ataques y la selección de objetivos cada vez más estratégicos plantean serios desafíos a la estabilidad internacional y la seguridad de los Estados occidentales.

Palavras-chave: Hacktivismo, APTs, ciberproxies, ciberconflito, ciberataques.

Palabras clave: Hacktivismo, APT, ciberproxies, ciberconflicto, ciberataques.

ABREVIATURAS

APT: *Ameaça Persistente Avançada.*

DDoS: *Ataque de negação de serviço distribuído.*

DOJ: *Departamento de Justiça dos EUA.*

FBI: *Federal Bureau of Investigation.*

GRU: *Direção Principal de Informações da Rússia (Glavnoe Razvedyvatel'noe Upravlenie).*

ICS: *Sistemas de Controlo Industrial.*

IRGC: *Corpo de Guardas da Revolução Islâmica do Irão.*

Exército informático da Ucrânia: *Exército informático da Ucrânia.*

NSA: *Agência de Segurança Nacional dos EUA.*

PMC: *Empresa Militar Privada.*

PSOA: *Private Setor Offensive Ator.*

SCADA: *Controlo de Supervisão e Aquisição de Dados.*

Stuxnet: *Nome do malware utilizado na operação "Jogos Olímpicos".*

1. INTRODUÇÃO

A guerra na Ucrânia fez com que o mundo ocidental fosse mais uma vez confrontado com o impacto do realismo político. Antes da invasão de 2022, a grande maioria dos analistas ocidentais era incapaz de imaginar um conflito convencional na cena internacional como o que continua a ocorrer às portas da Europa. Cegos pelas doutrinas do soft power e seguindo os paradigmas liberais da paz capitalista ou da teoria da paz comercial, os líderes europeus ignoraram deliberadamente o facto de que, em algumas partes do mundo, o realismo político ainda prevalece.

Num mundo cada vez mais digitalizado, onde existe uma interconexão virtual entre o plano intangível da tecnologia da informação e o próprio espaço físico, não é surpreendente que o atual inimigo da Europa represente um desafio de segurança. À medida que os Estados se tornaram cada vez mais dependentes das tecnologias da informação, também aumentaram as oportunidades para os actores hostis (estatais e não estatais) influenciarem o ambiente político e geopolítico através de acções no ciberespaço.

A guerra na Ucrânia não só marcou o início de uma operação de assédio e de perturbação cibernética por parte de ciberameaças ligadas ao Kremlin, como também provocou uma mudança no panorama hacktivista mundial: o que até há não muitos anos era o bastião da defesa da liberdade de expressão, da privacidade, da justiça social e dos direitos humanos, é agora uma ferramenta com implicações estratégicas e, em muitos casos, ligada direta ou indiretamente a governos e serviços secretos.

O ativismo digital ideológico e orientado para o protesto que os Anonymous outrora representaram está a evoluir para um fenómeno constituído por uma miríade de grupos nacionalistas que recorrem repetidamente a ataques distribuídos de negação de serviço (DDoS) para criar um clima de tensão e perseguição persistente dos inimigos ocidentais.

O hacktivismo tornou-se uma ferramenta de dois gumes. Por um lado, representa uma forma de expressão e de luta pela justiça social, pela transparência e pelos direitos humanos. Por outro lado, tornou-se uma arma utilizada pelos Estados para desenvolver campanhas de desestabilização política e de desinformação.

A utilização de ciberataques para fins geopolíticos pôs em evidência a linha ténue entre o ativismo e a cibercriminalidade patrocinada pelo Estado. Este artigo procura analisar a evolução do hacktivismo e a sua relação com os governos, bem como o papel dos grupos de Ameaças Persistentes Avançadas (APT) na utilização do ciberespaço para fins políticos e militares.¹

Através de uma análise de casos concretos, será explorada a colaboração (ou instrumentalização) dos hacktivistas pelos Estados, as implicações desta prática e o seu

¹ Grupos de ciberatacantes frequentemente associados a Estados-nação ou a grandes organizações criminosas, altamente sofisticados e persistentes, que se infiltram nas redes durante longos períodos de tempo para espionagem ou sabotagem e que dispõem de recursos abundantes (técnicos, económicos) para atacar alvos de elevado valor (governos, grandes empresas) com premeditação e furtividade.

impacto na geopolítica atual. Por fim, será feita uma reflexão sobre o futuro do hacktivismo num mundo cada vez mais interligado, onde a inteligência artificial e outras tecnologias emergentes poderão redefinir o papel destes actores no ciberespaço.

O hacktivismo já não é apenas um fenómeno marginal de protesto digital, mas um potencial risco de segurança para os Estados. Compreender a sua evolução e implicações é fundamental para analisar o futuro da cibersegurança espanhola.

2. DO PROTESTO SOCIAL À GUERRA CIBERNÉTICA

O hacktivismo sofreu uma transformação notável desde as suas origens, passando de uma forma de protesto social a uma ferramenta utilizada pelos governos para apoiar uma agenda política. Se pensarmos bem, esta transformação trai as origens e a própria essência do ativismo, e é por isso que, antes de analisarmos o papel desempenhado pelo hacktivismo como uma ferramenta ao serviço do Estado, acreditamos que é necessário olhar para a forma como este fenómeno evoluiu desde as suas origens.

Em certas abordagens contemporâneas, nomeadamente as orientadas para a sistematização terminológica, existe uma tendência para estabelecer uma relação hierárquica entre ciberactivismo e hacktivismo, entendendo o primeiro como um fenómeno mais amplo e englobando necessariamente o segundo como uma manifestação específica ou variante radicalizada. Esta leitura, presente tanto na literatura popular como em alguns quadros analíticos normativos, considera que o ciberactivismo representa a utilização das tecnologias digitais para a promoção de causas sociais, políticas ou culturais através de campanhas de sensibilização, petições em linha ou protestos virtuais. O hacktivismo, por outro lado, caracteriza-se pela utilização de ferramentas de hacking - como ataques distribuídos de negação de serviço (DDoS), violações de dados ou alteração de sítios Web - para fins semelhantes, embora por meios mais perturbadores ou mesmo ilícitos.

No entanto, esta interpretação, embora generalizada, é problematicamente reducionista e não resiste a um exame mais atento da teoria histórica e crítica dos movimentos digitais. Em primeiro lugar, o pressuposto de uma evolução linear e progressiva - do ciberactivismo "moderado" ao hacktivismo "radical" - ignora as trajetórias históricas distintas dos dois conceitos. O hacktivismo, longe de ser uma derivação tardia do ciberactivismo, surge simultaneamente e até mais cedo em certos contextos, com raízes na cultura hacker das décadas de 1980 e 1990, e articulado em torno de princípios como a liberdade de informação, o acesso aberto ao conhecimento e a desobediência civil no ciberespaço (Jordan & Taylor, 2004; Coleman, 2014).

De facto, o termo "hacktivismo" surge da combinação etimológica de "hacker" e "ativismo", descrevendo a utilização de conhecimentos informáticos para promover causas políticas ou sociais; e as suas raízes remontam a meados da década de 1990, quando grupos como o "*Culto da Vaca Morta*" (uma referência ao matadouro do Texas onde o grupo realiza as suas reuniões) defendiam o acesso universal à informação em linha como um direito humano fundamental e a luta contra governos opressivos.²

² O sítio Web de "O Culto da Vaca Morta" pode ainda ser consultado em: <https://cultdeadcow.com/about.html>

"*Cult of the Dead Cow*", considerado um dos fundadores do hacktivismo moderno, não só divulgou manifestos críticos do controlo estatal e empresarial da Internet, como também desenvolveu ferramentas com uma clara vocação disruptiva. Entre elas está o *Back Orifice* (1998), um software concebido para expor vulnerabilidades no sistema operativo Windows e denunciar deficiências na privacidade dos utilizadores³. Um ano mais tarde, em 1999, vários dos seus membros promoveram o projeto *Hacktivismo*, um ramo explicitamente orientado para a luta contra a censura digital que deu origem ao desenvolvimento de ferramentas como o *Six/Four* ou o *Peekabooby*, concebidas para contornar os filtros impostos por regimes autoritários e facilitar o livre acesso à informação.

Na ideologia do *Culto da Vaca Morta*, o acesso à informação online não era apenas um direito fundamental, mas também um campo de contestação política que exigia formas inovadoras de intervenção técnica e simbólica. No entanto, estas acções, embora não violentas em termos físicos, implicavam um confronto direto com a legislação restritiva sobre a utilização da rede e a propriedade intelectual; por outras palavras, revelavam o carácter ambíguo do hacktivismo.

Por outro lado, concetualizar o hacktivismo como uma simples intensificação tática do ciberactivismo faz-nos perder de vista as divergências ideológicas e epistemológicas entre ambos. Enquanto o ciberactivismo tende a enquadrar-se na lógica da participação dos cidadãos, da advocacia institucional e da utilização estratégica das redes sociais, o hacktivismo opera frequentemente através do antagonismo direto, da resistência às estruturas de poder e do questionamento dos quadros legais existentes.

Embora possa ser útil pensar o hacktivismo como uma subcategoria do ciberactivismo a partir de certas abordagens descritivas, é epistemologicamente insuficiente e empiricamente questionável quando se aborda a genealogia, o enquadramento normativo e as implicações ético-políticas de ambas as formas de ativismo digital. Neste artigo, centrar-nos-emos apenas na evolução do hacktivismo, entendido como um fenómeno em si mesmo, deixando de lado a formulação de uma revisão crítica desta classificação.

Nas fases iniciais do hacktivismo, o principal objetivo era levar a cabo ataques contra entidades governamentais e empresariais como forma de protesto contra a censura e as injustiças sociais. Estas mensagens tornaram-se mais intensas à medida que o movimento anti-globalização de meados da década de 1990 emergiu na cena social (Auty, 2004).

Um marco fundamental na consolidação do hacktivismo como ferramenta de confronto político foi a guerra do Kosovo, na década de 1990 (frequentemente descrita como a primeira guerra travada em linha), em que os contendores não só partilharam informações e testemunhos sobre a guerra em linha, como também difundiram propaganda e desinformação. Os *hackers* chegaram mesmo a intervir ativamente no conflito, desfigurando sítios Web do governo e executando ataques de negação de serviço contra as infra-estruturas em linha do lado oposto (Denning, 2001).

³ Embora inicialmente concebida como uma ferramenta de auditoria de segurança, a sua criação gerou alguma controvérsia e foi vista como uma ameaça pela indústria tecnológica.

Académica e socialmente, os movimentos hacktivistas eram vistos como a expressão natural de um ativismo político pré-existente que tinha encontrado numa nova ferramenta (a Internet) a possibilidade de empregar um tipo de ativista com um perfil técnico para difundir as suas mensagens de uma forma mais mediática (Jordan, 2002).

No entanto, o manifesto desrespeito pelas normas estabelecidas, as designações escolhidas pelos grupos (*The Legion of Doom*, *Bad Ass Mother Fuckers*, *Toxic Shock*, etc.) e o contexto de insegurança social aberto pelos atentados de 11 de setembro, fizeram com que um fenómeno que inicialmente era visto de forma positiva começasse a suscitar alguma desconfiança. (Torres Soriano, 2018).

A figura do *hacker* começou a ser identificada com a do criminoso e, por extensão, num contexto geopolítico marcado pela luta contra o Terror, com a do ciberterrorista. E as acções hacktivistas passaram a ser identificadas fundamentalmente como uma nova forma de participação política ilegítima, recorrendo a ciberataques para levar a cabo sabotagem e ciberespionagem (Vegh, 2005).

No plano académico, a identificação do hacktivismo com o ilegal ou criminalizável, frequente em certos discursos, reduz o hacktivismo a uma "forma radical de ciberativismo", empobrecendo assim a capacidade de análise e explicação das ciências sociais face à complexidade das práticas políticas digitais contemporâneas.

O início desta década reflecte um hacktivismo marcado pelo desejo dos seus membros de transgredir as convenções sociais por prazer. De facto, as raízes do grupo hacktivista mais conhecido (Anonymous) remontam ao fórum japonês *2chan*, onde a comunidade virtual se dedicava a partilhar todo o tipo de conteúdos aberrantes relacionados com anime, pornografia e piadas práticas (Bartlett, 2015).

No entanto, por volta de 2003, surgiram as primeiras tensões internas numa comunidade virtual que tinha encontrado no fórum *4chan* o local ideal para se divertir sem se importar com as consequências. Precisamente neste fórum, alguns utilizadores (conhecidos como *moralfags*) propuseram concentrar as suas actividades em causas mais transcendentais, como a luta contra a censura na Internet, para limpar a imagem do hacktivismo e representar a defesa da liberdade de expressão, da transparência e de outros direitos civis.

Sob o lema "*Somos Anónimos. Somos a Legião. Nós não perdoamos. Nós não esquecemos. Esperem por nós*" e a máscara de Guy Fawkes, surgiu um coletivo descentralizado de activistas que combinou a exfiltração de informação e os ataques DDoS para reivindicar a luta contra a corrupção, a censura e os abusos de poder.

Por parte do poder, o Anonymous foi rapidamente interpretado como uma premonição do risco representado por uma nova geração de actores virtuais motivados, com uma estrutura sem líderes e uma operação baseada no voluntarismo e na espontaneidade (Olson, 2012). No entanto, só quando o coletivo começou a apoiar as acções da WikiLeaks é que o grupo passou a ser visto como uma ameaça cibernética de alto nível.

Em pouco tempo, os Anonymous passaram de um pequeno grupo de *hackers* com ideias políticas para um movimento global com milhares de seguidores em todo o mundo.

No entanto, a sua atração não residia numa ideologia estruturada ou num programa de ação definido. Para além da sua posição anti-establishment, que os levou a denunciar a manipulação e o controlo exercidos pelos governos e pelas empresas, a sua filosofia carecia de uma orientação clara sobre a forma como a política, a sociedade ou a economia deveriam ser organizadas. Isto fez do Anonymous um fenómeno difícil de classificar, uma vez que a sua identidade se baseava mais na ação e no protesto do que numa agenda concreta para a mudança (Torres Soriano, 2018).

Sob a máscara de Guy Fawkes reuniram-se indivíduos que certamente acreditavam apoiar uma mudança social positiva, mas também outros: aqueles cuja inspiração era a destruição niilista do mundo tal como o conhecemos e aqueles que procuravam esconder-se sob a bandeira do Anonymous para obter ganhos políticos ou económicos.

Do principal legado dos Anonymous - transformar o hacktivismo numa prática popular que transcendeu a esfera *dos hackers* - surge uma nova era de hacktivistas que operam numa paisagem de fragmentação e complexidade, onde coexistem múltiplos actores com motivações diversas.

Atualmente, embora grupos como os Anonymous continuem a operar de forma descentralizada, o seu impacto diminuiu em comparação com o boom que atingiram no início da década de 2010. Ao mesmo tempo, surgiram novas gerações de hacktivistas que, embora tenham um nível inferior de conhecimentos técnicos, compensam com a utilização de ferramentas de automatização e um domínio do impacto mediático e da mobilização social.

Atualmente, o hacktivismo é utilizado tanto por colectivos independentes que denunciam a injustiça como por grupos patrocinados pelo Estado que instrumentalizam estas táticas para fins geopolíticos. O conflito entre a Rússia e a Ucrânia pôs em evidência a existência de uma guerra cibernética, com hacktivistas pró-ucranianos e pró-russos a levarem a cabo ataques coordenados em benefício dos respectivos lados.

A fronteira entre o ativismo digital legítimo, o cibercrime e as operações secretas dos serviços secretos é cada vez mais ténue. No entanto, podemos considerar que existem atualmente três tipos de hacktivistas: os ciberterroristas, os *hackers* cívicos e os *hackers* patrióticos (Dahan, 2013; Denning, 2001; Johnson e Robinson, 2014; Sauter, 2013).

O ciberterrorismo incluiria todas as acções hostis no ciberespaço destinadas a perpetrar actos de violência contra pessoas ou bens, com o objetivo de intimidar ou coagir governos ou sociedades a atingir fins políticos, religiosos ou ideológicos específicos. As suas acções envolvem principalmente a propagação de vírus e *malware*, a vandalização de *sítios Web* e a realização de ataques de negação de serviço (DDoS) ou *botnet* (Denning, 2001; Jordan e Taylor, 2004; Goode, 2015).

Na categoria de *hackers* cívicos encontraríamos todos os grupos organizados que realizam acções contra sistemas informáticos com o objetivo de contribuir com algum bem para a comunidade, geralmente na fronteira da legalidade (Hunsinger e Schrock, 2016; Schrock, 2016).

Por último, os *hackers* patrióticos são os indivíduos ou grupos cujos esforços estão alinhados com a ideologia nacionalista e são considerados uma "milícia cibernética" em busca de interesses específicos (Dahan, 2013; Green, 2016). Embora de fora estes *hackers* possam não parecer diretamente patrocinados por qualquer Estado, podemos agora inferir que são instrumentalizados como parte de uma rede mais vasta de forças estatais.

O *hacktivismo* patriótico teve origem na China, na década de 1990, em resposta a motins anti-chineses na Indonésia e, desde então, tem sido utilizado como tática pela China, Rússia, Síria e outros Estados como forma de prejudicar os seus inimigos no domínio cibernético. No entanto, nenhuma das operações anteriores à guerra da Ucrânia atingiu a escala, o impacto e os laços governamentais tão robustos e prolongados, nem transgrediu de forma tão flagrante as normas internacionais, como o *hacktivismo* contemporâneo (Healey & Grinberg, 2022).

3. O NEXO ENTRE O HACKTIVISMO E A APT

Ao longo da história, os Estados têm recorrido a actores por procuração para levar a cabo as suas estratégias de conflito sem envolver diretamente as suas forças armadas. Unidades auxiliares, grupos mercenários, insurreições, organizações terroristas ou empresas militares privadas (PMC) são apenas algumas das formas que os terceiros actores assumiram para substituir a ação estratégica dos Estados.

Por isso, não é de estranhar que hoje, perante uma sociedade cada vez mais digitalizada, a ação do Estado tenha encontrado nos grupos *hacktivistas* um novo ator para personificar a exteriorização da autoria e no ciberespaço o ambiente ideal para projetar influência geopolítica.

O conceito de *guerra de substituição* tem sido objeto de um amplo debate na comunidade académica e de segurança, sobretudo devido à dificuldade de o diferenciar da guerra *por procuração*, dada a natureza intimamente ligada dos dois conceitos.

Em ambos os casos, os objectivos do ator principal (o Estado) e do agente substituto coincidem. No entanto, enquanto na *guerra por procuração* existem dois ou mais atores hierarquicamente relacionados (o ator principal trabalha para, com e através do ator por procuração para atingir um objetivo comum), na *guerra de substituição* estes atores só estão alinhados se o ator principal conseguir mobilizar o apoio adequado exigido pelo ator por procuração (Fox 2019). Por outras palavras, os conceitos de *guerra de substituição* e de *guerra por procuração* diferem consoante a relação entre os atores e as suas motivações.

Uma vez que os grupos *hacktivistas* têm pouca independência para resistir ao controlo do Estado que os patrocina (ou que, pelo menos, os influencia ou tolera), no nosso estudo de caso falaremos em termos de actores *por procuração*.

Mais especificamente, para nos referirmos a eles, utilizaremos a definição de "proxy actors" de Rondeaux e Sterman (2019), que os definem como "*sujeitos fora da estrutura de segurança dos Estados envolvidos num conflito que agem sob o patrocínio direto ou indireto de um ator convencional (um Estado)*"; e a definição de Maurer (2018) de *cyber proxies* como "*intermediários que realizam acções ofensivas no ciberespaço em benefício de um ator principal*".

Historicamente, os *ciberproxies* têm sido personificados através de várias entidades ligadas ao mundo da cibercriminalidade e da ciberespionagem. No entanto, o termo engloba um grande número de entidades organizadas que, direta ou indiretamente, constituem um fator de risco para as empresas e os Estados. De facto, a lista de actores é muito extensa: grupos criminosos, *actores ofensivos do sector privado* (PSOA), grupos terroristas, insurrectos, insurgentes, hacktivistas, actores estatais ou APTs são apenas alguns deles.

As razões subjacentes à sua utilização são variadas: (1) a utilização de actores *por procuração* pelos governos reduz o risco de escalada dos conflitos, uma vez que a dificuldade de atribuir a responsabilidade por um ciberataque é complexa; (2) existe a possibilidade de uma negação plausível que desvia a responsabilidade de um ataque para um ator fora do controlo do governo; (3) ajuda os Estados a prolongar a situação de tensão nos conflitos, desgastando o adversário a nível social, político e económico; (4) permite que os Estados actuem à margem das regulamentações internas e das críticas de sectores governamentais adversários - ou mesmo da própria opinião pública nas democracias; (5) dá aos Estados rapidez e flexibilidade na resposta às acções ofensivas dos seus adversários, uma vez que não requer provas técnicas ou legitimação pública; (6) oferece aos Estados um instrumento adicional de dissuasão; (7) permite aos Estados contornar a aplicação do direito internacional; (8) facilita a utilização de pessoal especializado sem a necessidade de oferecer recrutamento legal; (9) possibilita a participação em conflitos internacionais que, de outra forma, seriam económica e politicamente incontrolláveis (Torres Soriano, 2017; Expósito Guisado, 2024; Marín Gutiérrez, 2023).

No entanto, a obtenção destes benefícios não é isenta de problemas. De facto, o principal atrativo da utilização de um *proxy* (que não é outro senão a obtenção de uma negação plausível de uma agressão) é também a sua principal fraqueza, uma vez que o anonimato e a clandestinidade diluem a capacidade coerciva e dissuasora do Estado patrocinador - afinal, não podemos ignorar as teorias de Clausewitz que sugerem que para um Estado modificar a sua conduta com base na vontade de outro, este último tem de conhecer a origem do ato de coerção a que foi submetido.

Outro inconveniente da utilização de *ciberproxies* reside na forma como o Estado os seleciona e controla quando são utilizados. A existência de interesses divergentes entre as duas partes pode levar à deslealdade do *proxy*, causando prejuízos económicos ou políticos ao ator que o utiliza - facto que é agravado se tivermos em conta que estes *proxies* operam geralmente em áreas onde o Estado não pode nem quer intervir.

A vantagem dos *mandatários* reside na sua capacidade de atuar de forma dissimulada, embora seja precisamente esta falta de transparência que limita o patrocinador estatal na verificação dos seus antecedentes e fiabilidade. A literatura académica salienta que o controlo sobre os *mandatários* é ainda mais complicado se o Estado não dispuser de mecanismos eficazes para sancionar a deslealdade, ou se existirem estruturas descentralizadas que impeçam a aplicação adequada de ordens hierárquicas (Popovic 2015).

Neste artigo, vamos concentrar-nos apenas em dois actores que representam os dois pólos diferentes (ativismo aberto e espionagem silenciosa) do mesmo fenómeno, mas que não são assim tão diferentes em termos dos fins que perseguem e da sua instrumentalização pelos Estados.

Em termos gerais, o hacktivismo e as APT diferem em termos de motivação, métodos e grau de apoio estatal. Assim, enquanto o hacktivismo é motivado por um contexto político-social (protesto, ativismo, causas morais), as APT centram-se na espionagem estratégica e na obtenção de uma vantagem económico-militar.

Operacionalmente, as APT actuam de forma furtiva e persistente, recorrendo a *malware* personalizado, backdoors e movimentos laterais, ao contrário das acções de hacktivismo, que normalmente procuram chamar a atenção do público e se concentram em ataques DDosS de curta duração.

No entanto, não é raro observar como as APT actuam temporariamente como hacktivistas (quando divulgam publicamente os dados que exfiltram para provocar um impacto político) e como os hacktivistas são instrumentalizados pelos Estados para atingir os seus objectivos estratégicos.

A nível organizacional, os hacktivistas e as APT também diferem: os hacktivistas agem geralmente de forma descentralizada, espontânea, mesmo anónima, e sem um comando unificado. As APT, por outro lado, são geralmente equipas estruturadas, muitas vezes integradas numa organização maior (um exército, uma agência de informações ou um grupo criminoso), com uma hierarquia definida e um financiamento consideravelmente mais poderoso (CyberZaintza, 2021).

De facto, a diferença de recursos e de formação técnica sugere uma ligação mais estreita entre as APT e os Estados do que entre os grupos de hacktivistas. No entanto, as linhas que separam os dois conceitos foram recentemente esbatidas pela constatação de que alguns grupos de hacktivistas pró-russos têm recebido apoio estatal encoberto ou actuam de acordo com a agenda do Estado, esbatendo a distinção até agora clara entre "*hackers* activistas" e "agentes do Estado" (Muncaster, 2024).

De facto, não se pode excluir que certos grupos de hacktivistas sejam realmente formados ou apoiados por APT ou diretamente por actores estatais. Um exemplo é o "XakNet Team", o "Infocentr" e o "CyberArmyofRussia_Reborn", grupos hacktivistas pró-russos que, segundo a Mandiant, são agentes de ciberameaças patrocinados pela Direção Principal dos Serviços Secretos russos (GRU) através da APT44 (Mandiant, 2022).

Na última década, foram documentados vários casos em que os Estados utilizaram os seus próprios grupos APT e colectivos de hacktivistas (ou as suas identidades) para levar a cabo ciberespionagem, sabotagem de conflitos e manipulação política.

Um exemplo paradigmático que ilustra a interdependência de ambos os conceitos pode ser encontrado nas eleições de 2016 nos EUA, quando "*DCLeaks*" e "*Guccifer 2.0*", duas identidades ligadas à Direção Principal de Inteligência da Rússia (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), roubaram e-mails do Partido Democrata e os divulgaram fazendo-se passar por "hacktivistas patrióticos americanos" (DOJ, 2018).

No rescaldo da guerra na Ucrânia, não é raro encontrar interdependência entre hacktivistas russos e APT, grupos como *Killnet*, *NoName057(16)*, *Anonymous Sudan* que atacaram sítios Web governamentais e empresas ocidentais em apoio da narrativa do Kremlin mostram que, embora estes grupos se autodenominem "activistas espontâneos",

agem de forma suspeita em coordenação com a ação do Estado russo (Van Der Walt, 2025).

No entanto, a Rússia não é o único ator estatal que recorre às APT e aos hacktivistas para fazer valer o seu poder. Há anos que outros Estados, como a China, a Coreia do Norte ou o Irão, são acusados de conduzir desta forma as suas actividades ofensivas no ciberespaço.

Concretamente, a China é acusada há anos de patrocinar vastas campanhas de ciberspionagem através de unidades militares e *hackers* pagos, como os do grupo APT1, considerado pela Mandiant em 2013 como a Unidade 61398 do Exército Popular de Libertação da China.

As operações APT chinesas tendem a centrar-se em alvos estratégicos (aeroespacial, energia, telecomunicações, defesa, etc.) e são consideradas parte dos serviços secretos do Estado chinês, mas, ao contrário da Rússia, o recurso ao hacktivismo não é tão proeminente nas estratégias chinesas.

O governo tolerou e até inspirou "*hackers* patrióticos" chineses em alguns conflitos, sendo um exemplo a "*Honker Hacker Network*", uma comunidade de *hackers* fora do controlo do governo - de acordo com fontes chinesas - que atacou actores adversários da China durante disputas territoriais ou incidentes diplomáticos.

O Irão, por outro lado, tem mostrado uma tendência para instrumentalizar grupos de *hackers* supostamente activistas para levar a cabo operações de retaliação contra os seus adversários, ao mesmo tempo que desenvolve as suas próprias APT. Um exemplo significativo deste facto foram os ataques DDoS contra bancos norte-americanos em 2012-2013, em retaliação contra as sanções ocidentais: uma entidade que se dizia hacktivista religiosa e se intitulava "*Cyber Fighters of Izz ad-Din al-Qassam*" reivindicou a autoria da ofensiva, invocando a indignação contra um vídeo anti-islâmico (CFR, 2012).

Os serviços secretos americanos concluíram posteriormente que se tratava de uma operação orquestrada pelo Irão (provavelmente a sua Guarda Revolucionária) em resposta às medidas tomadas contra o seu programa nuclear. De facto, em 2016, o Departamento de Justiça dos EUA indiciou sete iranianos ligados à Guarda Revolucionária Islâmica (IRGC) por estes ataques.

Outro exemplo é o ataque "*Shamoonj*" de 2012 do "*Cutting Sword of Justice*", um alegado grupo hacktivista que apagou dados de 30 000 computadores da empresa petrolífera saudita Aramco, mas que os analistas atribuíram mais tarde a uma operação estatal iraniana em resposta à ofensiva *Stuxnet* e às tensões regionais.

A Coreia do Norte, apesar do seu isolamento, também conseguiu criar uma das ciberameaças mais activas, principalmente para angariar fundos e desestabilizar os seus adversários geopolíticos. O seu grupo APT mais notável, o *Lazarus Group* (ligado ao APT38), roubou centenas de milhões através de ataques a bancos.

Outro caso que ilustra a instrumentalização de campanhas activistas pelos Estados pode também ser encontrado numa das suas acções, a *pirataria* informática da Sony Pictures em 2014, quando um grupo chamado "*Guardians of Peace*" exfiltrou dados

confidenciais e destruiu sistemas da Sony em aparente retaliação pelo filme satírico sobre o líder norte-coreano "*The Interview*". (FBI, 2014).

A Coreia do Norte é o paradigma da instrumentalização direta, os seus *hackers* são agentes do Estado que, por vezes, assumem os nomes de grupos fictícios para disseminar as suas mensagens ou justificar os seus ataques, mas, ao contrário de outros Estados, os norte-coreanos eliminam completamente a distinção entre APT e aparelho de Estado, mantendo a cobertura apenas na narrativa pública para o mundo exterior.

Por seu lado, as potências ocidentais também empregam, obviamente, capacidades cibernéticas ofensivas para atacar outros Estados. Talvez o caso mais relevante seja a operação "Jogos Olímpicos" atribuída às agências NSA e à unidade 8200 (não oficialmente reconhecida), na qual os EUA e Israel desenvolveram o malware *Stuxnet* para sabotar as centrífugas nucleares do Irão por volta de 2010 (The Guardian, 2017).

No entanto, no Ocidente, embora existam entidades APT apoiadas por Estados para atuar ofensivamente em campanhas de espionagem, a instrumentalização de grupos hacktivistas para esconder as suas acções é praticamente inexistente. De facto, só encontramos um caso em que um grupo hacktivista ocidental associa a sua atividade à capacidade ciber-ofensiva de um Estado: o "*IT Army of Ukraine*".

Este caso é particularmente controverso, uma vez que o apoio público do governo ucraniano viola abertamente as normas recentemente acordadas sobre a conduta dos Estados no ciberespaço, bem como as posições de política externa dos membros da NATO (Healey e Grinberg, 2022).

Se utilizarmos a tabela "Spectrum of Responsibility" de Healey e Grinberg (2022), que correlaciona a atividade dos grupos de acordo com o grau de responsabilidade do Estado pela sua *representação cibernética*, podemos ver como o apoio do governo ucraniano ao *IT Army of Ukraine* começou pelo menos como "coordenado pelo Estado (nível 6)", (quando o Ministro ucraniano da Transformação Digital, Mikhail Fedorov, apelou abertamente a voluntários hacktivistas de todo o mundo para apoiarem a Ucrânia na frente digital) e até "encorajado pelo Estado (nível 4)".

Quadro 1: Espectro da responsabilidade do Estado.

Posição do Estado	Relação Estado-Procurador
1. Proibido pelo Estado.	O governo nacional ajudará a travar uma ataque de terceiros.
2. Proibição estatal mas inadequada.	O governo nacional coopera, mas é incapaz de impedir o ataque de terceiros.
3. Ignorado pelo Estado.	O governo nacional está ciente dos ataques de terceiros, mas não está disposto a tomar nenhuma ação oficial.
4. Patrocinado pelo Estado.	Terceiros controlam e dirigem o ataque, mas o governo nacional promove-os como um questão política.
5. Moldado pelo Estado.	Terceiros controlam e dirigem o ataque, e o Estado presta algum apoio.
6. Coordenado pelo Estado.	O governo nacional coordena o ataque através de terceiros, por exemplo, sugerindo pormenores operacional.
7. Obrigatório pelo Estado.	O governo nacional ordena a terceiros que realizar o ataque em seu nome.
8. Gerido, mas não reconhecido pelo Estado.	Elementos fora do controlo das forças ataques cibernéticos do governo nacional levam a ataque ordenado.
9. Implementado pelo Estado.	O governo nacional efectua o ataque utilizando forças cibernéticas sob a sua controlo direto.
10. Integrado no Estado.	Ataques do governo nacional utilizando proxies e forças cibernéticas incorporadas governamental.

(Healey, 2022).

É sobretudo nos conflitos geopolíticos que vemos a convergência mais acelerada entre o hacktivismo e as operações estatais. No caso da guerra ucraniana, três anos após o início do conflito e apesar de o número de actores hacktivistas ter diminuído consideravelmente (de mais de 130 grupos em 2024 para apenas cerca de 80 grupos em 2025), podemos ainda observar como ambos os lados mantêm um cruzamento de ciberataques destrutivos, coordenados com a sua campanha militar e apoiados nas suas acções por "hackers patrióticos" (Cyberknow, 2025).

Do lado ucraniano, o *IT Army of Ukraine* continua a ser a força hacktivista mais importante da Ucrânia, continuando a mobilizar voluntários dentro e fora do país para atacar infra-estruturas russas, realizar contra-propaganda e apoiar missões de informação. No período de 2023-2024, é-lhe atribuída, por exemplo, a tarefa de derrubar temporariamente os serviços de Internet nas zonas ocupadas pela Rússia e de lançar continuamente campanhas de DDoS contra entidades russas de alto nível (Optiv, 2023).

Do lado pró-russo, o grupo mais proeminente neste momento é o *NoName057(16)*, um grupo ligado ao GRU, que actua em coordenação com a agenda do Kremlin,

selecionando alvos de acordo com os interesses estratégicos russos e considera-se uma espécie de "braço ciberespontâneo" permanente dos militares russos.

Quadro 2: *Casos cronológicos de instrumentalização do hacktivismo pelo Estado.*

Ano	Estado	Grupo hacktivista	Caraterística	Nível de ligação ao Estado (Healey & Grinberg).
1998-1999	Kosovo	Hackers patriotas	Primeiro conflito com uma intervenção notável de hacktivistas.	Ignorado / Espontâneo
1999	China	Buzina vermelha	Hackers patrióticos activos em conflitos territoriais. Campanhas de espionagem industrial e ciberataques a infra-estruturas críticas.	Incentivado / Moldado
2012-2013	Irão	Combatentes cibernéticos do Izz ad-Din al-Qassam	Ataques DDoS contra bancos americanos em retaliação às sanções. Operação Shamoon contra a Aramco com eliminação em massa.	Coordenado / Ordenado
2014	Coreia do Norte	Grupo Lazarus	Ciberataques para obter financiamento estatal. Ataque à Sony Pictures (2014) como retaliação simbólica.	Implementado / Integrado
2022-presente	Rússia	Killnet/Cyber Army of Russian Reborn/NoName057(16)	Os grupos hacktivistas coordenaram-se com a estratégia russa na guerra da Ucrânia. Ataques DDoS.	Coordenado / Incentivado
2022-presente	Ucrânia	Exército informático da Ucrânia	Apelo público do Governo ao hacktivismo contra a Rússia. DDoS, sabotagem e propaganda pró-ucraniana.	Coordenado / Incentivado

4. O FUTURO DOS GRUPOS HACKTIVISTAS.

A sobrevivência dos grupos de hacktivistas indica que o hacktivismo integrado na guerra veio para ficar, pelo menos enquanto durar o conflito subjacente e os Estados em conflito

considerarem útil esta camada de ação descentralizada. Além disso, o panorama atual dos hacktivistas leva-nos a observar que o hacktivismo está a ir além do DDoS e a entrar em ataques APT mais sofisticados, como os ataques a infra-estruturas críticas SCADA e a sistemas de controlo industrial (ICS) .⁴

O facto de grupos pertencentes ao ecossistema hacktivista pró-russo, como a *Z-Pentest Alliance* ou o *Setor 16*, terem vindo a intrometer-se ativamente em centrais eléctricas, instalações de água potável e indústrias em geral, reflecte não só uma maturação e uma estadualização do fenómeno hacktivista, mas também a existência de riscos físicos crescentes das suas acções (Antoniuk, 2024).

A redução do número de grupos hacktivistas no ambiente pró-russo sugere que a efervescência inicial deu lugar a um processo de seleção natural em que sobrevivem os grupos com melhor apoio, organização e proteção. Um fenómeno que se traduz em operações mais eficazes e coordenadas, mas também mais previsíveis, uma vez que estão alinhadas com a agenda do Estado russo.

Ao mesmo tempo, a persistência de ataques diários indica que a guerra cibernética de baixa intensidade se tornou uma rotina. O DDoS constante mantém a pressão psicológica e de propaganda sobre as populações-alvo (lembretes diários da presença do conflito), enquanto a adoção de *ransomware* e os ataques a indústrias aumentam o potencial de danos reais a infra-estruturas críticas, esbatendo a linha entre o hacktivismo e o ciberterrorismo - um facto que pode, em última análise, levar a respostas mais enérgicas por parte dos Estados vítimas e a uma potencial escalada do conflito.

Outro desenvolvimento relevante é o desenvolvimento notável de alianças emergentes entre causas hacktivistas que transcendem o teatro de operações para além da Ucrânia e envolvem países terceiros. Um exemplo é a recente aliança entre hacktivistas pró-russos e pró-palestinianos, que une causas geopolíticas aparentemente distintas sob uma narrativa comum de ataque ao Ocidente.

As tensões globais de 2024 (incluindo a guerra de Gaza) criaram uma estranha frente unida de hacktivistas. Grupos russos (especialmente *NoName057(16)*) começaram a coordenar operações com colectivos ligados ao Médio Oriente (como *Mr. Hamza* ou *Anonymous Guys*) e sincronizaram os seus ataques sob a bandeira da união da "*Santa Liga*" contra países que consideravam adversários comuns, como a França.

Este tipo de aliança é bem conhecido em Espanha, e particularmente pela Guardia Civil, uma vez que, em julho de 2024, a instituição foi o alvo direto de uma campanha conjunta de ciberataques, "*#FuckGuardiaCivil*", que respondeu a uma iniciativa promovida pelo grupo *NoName057(16)*, para "se vingar das autoridades espanholas" que tinham detido três pessoas em Manacor (Maiorca), Huelva e Sevilha por suspeita de participação em ciberataques contra entidades públicas e empresas estratégicas em Espanha e noutros países da NATO.

⁴ Sistema centralizado para monitorizar, controlar e recolher dados de processos e dispositivos em tempo real.

De facto, em abril de 2025, já estava registada uma nova aliança, incluindo os grupos *Keymous+*, *Mr Hamza*, *Alixsec* e *NoName057(16)*, para atacar a Polónia, a Alemanha, a França, a Itália e a Espanha sob o lema "*Operação Hack For Humanity V2!*"

Só em Espanha, no primeiro dia da campanha "*Operação Hack For Humanity V2!*", foram registados mais de 30 ataques a empresas e sítios Web governamentais, sendo o *Sr. Hamza*, o *NoName057(16)*, o *TwoNet* e o *Keymous+* os grupos mais activos no ataque.

A frequência com que esta convergência tem vindo a ocorrer nos últimos meses mostra que o fenómeno está a tornar-se cada vez mais internacional e interligado. As alianças entre grupos hacktivistas tornaram-se solidárias, transcendendo as fronteiras do conflito russo-ucraniano com um único objetivo: expandir as suas acções para o inimigo comum ocidental.

O facto de países da NATO como a França, a Itália ou a própria Espanha se poderem tornar alvos de *piratas* informáticos patriotas russos pode levar a uma escalada do conflito, especialmente se um dos seus ataques danificar gravemente infra-estruturas críticas, a guerra cibernética de baixa intensidade pode atrair uma resposta mais forte do que o habitual.

5. CONCLUSÕES

A análise do hacktivismo e da sua relação com os Estados mostra que este fenómeno evoluiu do protesto digital para uma instrumentalização estatal com implicações geopolíticas e estratégicas. A fronteira entre ativismo, cibercrime e operações estatais é cada vez mais ténue, especialmente em conflitos como a guerra na Ucrânia, onde se tem observado uma crescente instrumentalização de grupos hacktivistas por forças governamentais na defesa dos seus interesses nacionais.

Com efeito, o conflito entre a Rússia e a Ucrânia marcou um ponto de viragem na utilização do ciberespaço como campo de batalha, em que tanto os intervenientes estatais como não estatais se envolveram ativamente em ataques de negação de serviço (DDoS), ciberspionagem e sabotagem de infra-estruturas críticas.

Este estudo, desenvolvido através do estudo dos casos mais proeminentes na cena internacional, permitiu-nos estabelecer uma distinção entre *hackers* cívicos e *hackers* patrióticos. Enquanto os primeiros abraçam causas niilistas ou socialmente conflituosas, os segundos são utilizados pelos Estados como um instrumento encoberto nos conflitos internacionais, o que implica uma externalização das cibercapacidades governamentais e oferece uma série de vantagens estratégicas: negação plausível de responsabilidades, prolongamento de situações de tensão ou redução de custos políticos e económicos.

Em suma, poderíamos dizer que os Estados aprenderam a explorar o hacktivismo como uma arma adicional, quer fingindo ser hacktivistas para desinformar ou exfiltrar dados, quer encorajando os seus simpatizantes a lançar ciberataques em massa contra o seu inimigo.

No entanto, esta instrumentalização coloca sérios desafios a nível estratégico. A sofisticação progressiva dos ataques, que passaram do vandalismo digital para operações mais avançadas contra infra-estruturas críticas, só aumenta seriamente as possibilidades de retaliação por parte dos Estados afectados e aumenta o risco potencial de escalada em conflitos assimétricos.

Além disso, a convergência entre as APT e os hacktivistas põe em causa as normas internacionais existentes, uma vez que os ataques perpetrados por agentes *por procuração* esbatem a responsabilidade do Estado e dificultam a aplicação de medidas de dissuasão ou de retaliação direta. Tanto mais que os colectivos de hacktivistas parecem estar a evoluir para uma nova paisagem de alianças capazes de reunir grupos de hacktivistas com agendas geopolíticas diversas para atacar países ocidentais.

A cibersegurança do Estado tem de se adaptar a uma nova realidade em que os grupos hacktivistas desempenham um papel fundamental na projecção do poder do Estado. As democracias ocidentais, tradicionalmente mais relutantes em utilizar tais tácticas, enfrentam o dilema de como responder eficazmente sem comprometer os seus valores.

A tendência atual não só mostra uma clara evolução do hacktivismo no sentido de uma ligação cada vez maior aos interesses estatais do governo que o apoia, como também reforça a ideia de que o ciberespaço continuará a ser mais importante em conflitos futuros. Casos como o da Rússia, onde grupos como o *Killnet* ou o *NoName057(16)* reivindicaram operações cibernéticas coincidentes com os interesses geopolíticos do Kremlin - sobretudo durante a guerra na Ucrânia -, ou o do Irão, com grupos como o *Tapandegan*, cuja retórica oposicionista não impede suspeitas de coordenação indireta com agendas estatais, exemplificam esta deriva e demonstram um progressivo esbatimento entre actores não-estatais e estatais na esfera digital, onde o hacktivismo deixa de ser exclusivamente uma forma de dissidência cidadã para se tornar, em certos contextos, uma ferramenta informal de projecção do poder estatal.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- Antoniuk, D. (2024). *Cybervolk: Hacktivistas da Índia e da Rússia colaboram em ataques de ransomware*. The Record. <https://therecord.media/cybervolk-india-hacktivists-russia-ransomware>
- Antoniuk, D. (2024). *Cybervolk: Hacktivistas da Índia e da Rússia colaboram em ataques de ransomware*. The Record. <https://therecord.media/cybervolk-india-hacktivists-russia-ransomware>
- Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *Aslib Proceedings*, 56(4), 212-221.
- Bartlett, J. (2015). *The dark net: Inside the digital underworld*. Melville House.
- CFR (2012). *Ataques de negação de serviço contra bancos dos EUA em 2012-2013*. Conselho de Relações Exteriores (CFR). <https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013>
- Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.
- Cyberknow (2025). *Guerra Rússia-Ucrânia: Atualização dos hacktivistas*. <https://cyberknow.substack.com/p/russia-ukraine-war-hacktivist-update>
- CyberZaintza (2021). *Grupo APT*. <https://www.ciberseguridad.eus/ciberglosario/grupo-apt>
- Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. *Conferência Internacional sobre Guerra e Segurança da Informação*, 51-VII. Academic Conferences International Limited. <https://search.proquest.com/docview/1549245919>
- Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. Em J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.
- DOJ (2018). *Grande júri acusa 12 oficiais dos serviços secretos russos por crimes de pirataria informática relacionados com as eleições de 2016*. Departamento de Justiça dos EUA. <https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>
- Expósito Guisado, J. (2023). *Ciberproxies: APTs como um fator de risco futuro*. Instituto Espanhol de Estudos Estratégicos (IEEE). *Boletim IEEE*, (32), 815-831.
- FBI (2014). *Atualização sobre a investigação da Sony*. Federal Bureau of Investigation (FBI), Washington, D.C. <https://www.fbi.gov/news/press-releases/update-on-sony-investigation>

- Fox, A. C. (2019). *Conflito e a necessidade de uma teoria da guerra por procuração*. *Journal of Strategic Security*, 12(1), 44-71. JSTOR. www.jstor.org/stable/26623077
- Goode, L. (2015). Anonymous e o ethos político do hacktivismo. *Comunicação Popular*, 13(1), 74-86. <https://doi.org/10.1080/15405702.2014.978000>
- Green, K. (2016). A guerra do povo no ciberespaço: Utilização da economia civil da China no domínio da informação. *Military Cyber Affairs*, 2(1). <https://doi.org/10.5038/2378-0789.2.1.1022>
- Healey, J., & Grinberg, A. (2022). *Patriotic hacking: No exception*. Lawfare. <https://www.lawfaremedia.org/article/patriotic-hacking-no-exception>
- Hern, A. (2017). O contratante da NSA divulgou ferramentas de hacking dos EUA por engano, diz Kaspersky. *The Guardian*. <https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office>
- Hunsinger, J., & Schrock, A. (2016). A democratização do hacking e da criação. *New Media & Society*, 18(4), 535-538. <https://doi.org/10.1177/1461444816629466>
- Johnson, P., & Robinson, P. (2014). Civic hackathons: Inovação, aquisição ou envolvimento cívico? *Review of Policy Research*, 31(4), 349-357. <https://doi.org/10.1111/ropr.12074>
- Jordan, T. (2002). *Ativismo! Ação direta, hacktivismo e o futuro da sociedade*. Reaktion Books.
- Jordan, T., & Taylor, P. A. (2004). *Hacktivismo e guerras cibernéticas: rebeldes com uma causa?* Psychology Press.
- Mandiant (2022). *A ascensão do GRU: os lacaios do Telegram*. <https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions>
- Marín, F. (2023). *Hacktivismo ao serviço do Estado: ciberproxies na Ucrânia*. Documento de opinião. Instituto Espanhol de Estudos Estratégicos (IEEE).
- Maurer, T. (2018). *Cyber Mercenaries: The state, hackers, and power [Mercenários cibernéticos: o estado, os hackers e o poder]*. Cambridge University Press.
- Muncaster, P. (2024). *Hacktivismo: A evolução das ameaças às organizações*. WeLiveSecurity. <https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones>

- Olson, P. (2012). *5 coisas que todas as organizações podem aprender com o Anonymous*. Forbes. <http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/>
- OPTIV (2023). *Atualização Rússia/Ucrânia - dezembro de 2023*. <https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023>
- Popovic, M. (2015). Fragile proxies: Explaining rebelde defection against their state sponsors. *Terrorismo e Violência Política*. <https://doi.org/10.1080/09546553.2015.1092437>
- Rondeaux, C., & Sterman, D. (2019). *Twenty-first century proxy warfare: Confronting strategic innovation in a multipolar world since the 2011 NATO intervention*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf
- Sauter, M. (2013). "LOIC will tear us apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *American Behavioral Scientist*, 57(7), 983-1007. <https://doi.org/10.1177/000276>
- Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society*, 18(4), 581-599. <https://doi.org/10.1177/1461444816629469>
- Torres Soriano, M. (2017). Guerras por procuração no ciberespaço. *Revista do Instituto Español de Estudios Estratégicos*, (9), 15-36.
- (2018). O hacktivismo como estratégia de comunicação do Anonymous ao cibercalifado. *Cuadernos de Estrategia*, (197), 197-224.
- Van Der Walt (2025). *Reflexão sobre três anos de guerra cibernética na Ucrânia*. *ComputerWeekly*. <https://www.computerweekly.com/opinion/Reflecting-on-three-years-of-cyber-warfare-in-Ukraine>
- Vegh, S. (2005). *The media's portrayal of hacking, hackers, and hacktivism before and after September 11. First Monday*. <http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126>



Artigo de investigação

PROTECÇÃO INTERNACIONAL E SOBERANIA: O COMPLICADO EQUILÍBRIO ENTRE DIREITOS INDIVIDUAIS E SEGURANÇA NACIONAL

Tradução para o português com ajuda de IA (DeepL)

Alejandro Gómez García
Capitão da Guardia Civil
Mestrado em Gestão da Segurança Operacional
Licenciatura em Direito
alejandrogomezg@guardiacivil.es
ORCID: <https://orcid.org/0000-0003-0162-4213>

Recebido em 31/03/2025

Aceite em 28/04/2025

Publicado em 27/ 06/2025

Citação recomendada: Gómez, A. (2025). Proteção internacional e soberania: o complicado equilíbrio entre direitos individuais e segurança nacional. *Revista Logos Guardia Civil*, 3(2), p.p. 123-146.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

PROTECÇÃO INTERNACIONAL E SOBERANIA: O COMPLICADO EQUILÍBRIO ENTRE DIREITOS INDIVIDUAIS E SEGURANÇA NACIONAL

Resumo: ANÁLISE TEÓRICO-METODOLÓGICA: ESTADOS, FRONTEIRAS E PROTECÇÃO INTERNACIONAL. 2.1 Mapa concetual do ambiente fronteiriço. 2.2. 2.2 Migração e Asilo. 3. ANÁLISE JURÍDICA: POSIÇÕES OPOSTAS E REACÇÃO DOS TRIBUNAIS. 3.1. *O caso Hirsi Jamaa v. Itália*: a génese de uma doutrina. 3.2. *N. D. e N. T. contra Espanha*: os limites da protecção. 3.3 Análise comparativa: a compatibilidade de uma doutrina jurisprudencial díspar. 4. CONCLUSÕES.

Resumo: O presente artigo pretende analisar o atual estatuto jurídico de alguns dos conceitos mais relevantes no domínio da protecção das fronteiras nacionais, bem como o seu contexto sócio-político e alcance jurídico, com o objetivo último de apoiar e promover o desenvolvimento de um debate doutrinário tão aceso nas suas posições como complexo no seu contexto: assegurar um adequado equilíbrio entre a garantia dos Direitos Fundamentais dos indivíduos que atravessam as fronteiras europeias e o exercício dos poderes soberanos inerentes aos Estados. Assim, num primeiro momento, proceder-se-á a uma análise detalhada das noções mais importantes no domínio da segurança das fronteiras, estabelecendo o campo de estudo de um ponto de vista científico. De seguida, numa perspetiva jurídica, serão estudadas as implicações dos mais importantes pronunciamentos dos órgãos judiciais (fundamentalmente internacionais) que se debruçaram sobre a matéria, bem como a posição da doutrina e da prática internacionais. Por fim, à luz das análises apresentadas, será oferecida uma série de conclusões coerentes com os resultados obtidos.

Resumen: En el presente artículo se pretende analizar el estatus jurídico que ostentan, en la actualidad, algunos de los conceptos más relevantes dentro del ámbito de la protección de las fronteras nacionales, así como su contexto sociopolítico y su alcance jurídico, con el fin último de fundamentar e impulsar el desarrollo de un debate doctrinal tan candente en sus posturas como complejo en su contexto: Asegurar un adecuado balance entre la garantía de los Derechos Fundamentales de los individuos que transiten por las fronteras europeas y el ejercicio de las potestades soberanas consustanciales a los Estados. Así, en primer lugar, se realizará un examen pormenorizado de las nociones más importantes en el ámbito de la seguridad fronteriza, fijando el campo de estudio desde un punto de vista científico. Inmediatamente a continuación se estudiarán, desde una perspectiva jurídica, las implicaciones que han tenido los pronunciamientos más importantes efectuados por los órganos judiciales (fundamentalmente internacionales) que han entendido de la materia, así como la posición de la doctrina y la práctica internacional. Y finalmente, a la luz de los análisis expuestos, se ofrecerá una serie de conclusiones coherentes con los hallazgos efectuados.

Palavras-chave: Direito Internacional, Asilo, Soberania, Fronteiras, Imigração.

Palabras clave: Derecho Internacional, Asilo, Soberanía, Fronteras, Inmigración.

ABREVIATURAS

AN: Audiência Nacional

ANP: Autoridade Nacional Palestiniana

CDFUE: Carta dos Direitos Fundamentais da União Europeia

CEDH: Convenção Europeia dos Direitos do Homem

IMO: *Organização Marítima Internacional - Organização Marítima Internacional*

SAR: *Search and Rescue (Busca e Salvamento) - Busca e Salvamento*

SOLAS: *Proteção da vida humana no mar - Proteção da vida humana no mar*

TEDH: Tribunal Europeu dos Direitos do Homem

TIJ: Tribunal Internacional de Justiça

APC: Tribunal Permanente de Arbitragem

PCIJ: Tribunal Permanente de Justiça Internacional

UE: União Europeia

1. INTRODUÇÃO

Na sequência do Acórdão do Tribunal Europeu dos Direitos do Homem (doravante CEDH), Terceira Secção, de 3 de outubro de 2017, através do qual o Estado espanhol foi condenado, no âmbito da prática de "rejeição na fronteira", por violação do artigo 13.º da Convenção Europeia dos Direitos do Homem (doravante CEDH) e do artigo 4.º do seu Protocolo n.º 4, prevendo o pagamento de uma indemnização aos demandantes N. D. (nacional do Mali) e N.T. (nacional da Costa do Marfim) no valor de 5.000 euros cada um; foram muitas as vozes que apelaram a uma mudança total de rumo na política migratória desenvolvida pelo Reino de Espanha e, por extensão, na política migratória europeia. De facto, a notícia fez manchete na imprensa¹, bem como na imprensa, com declarações fortes de organizações não governamentais² e até de entidades de direito público³, num país que não está habituado a seguir a crónica judicial com tanto detalhe, e muito menos a nível internacional.

E a situação não era para ser encarada de ânimo leve. A crescente preocupação com o contexto migratório na União Europeia (doravante UE) tinha dado origem, ao longo dos anos, ao surgimento de alguns debates que, até então, tinham permanecido à margem das dinâmicas políticas, que aceitavam como algo quase anedótico o aumento sustentado do número de nacionais de países terceiros a residir na União, cujo número tinha aumentado mais de 10% nos três anos anteriores ao referido pronunciamento⁴. Naturalmente, a ascensão deste debate tinha sido também alimentada pela chamada "Crise dos Refugiados" de 2015, em que centenas de milhares de pessoas deslocadas do Médio Oriente (maioritariamente sírios) tinham entrado em território europeu em resultado da instabilidade e da guerra na região. E, definitivamente, não ajudaria a aliviar a tensão na sociedade europeia se alguns dos envolvidos em vários actos terroristas que ocorreram durante esses anos (por exemplo, os ataques de Ansbach e Berlim em 2016 ou, claro, os ataques de Paris de 2015) fossem posteriormente identificados como refugiados ou imigrantes ilegais, vindos da Síria através da rota do Mediterrâneo Oriental.

Mas, como se isso não bastasse, o futuro reservava uma nova grande surpresa que iria, mais uma vez, virar o guião da política europeia de migração de pernas para o ar. Num acontecimento sem precedentes, o mesmo TEDH que tinha anulado a doutrina espanhola sobre as rejeições nas fronteiras viria a reverter a sua decisão em primeira instância e, num acórdão da Grande Secção de 13 de fevereiro de 2020, passou a declarar, por uma maioria de 16 para 1, a plena legalidade das rejeições nas fronteiras. Depois veio a pandemia. E com ela veio a reativação da rota migratória atlântica para as Ilhas Canárias, bem como um novo boom de movimentos migratórios para a UE em geral, que passariam de 125.226 entradas ilegais detectadas em 2020 (Frontex, 2021, p. 14) para 380.227 em 2023 (Frontex, 2024, p. 1). Atualmente, a imigração ocupa um lugar predominante entre

¹ RTVE (3 de outubro de 2017), *O Tribunal Europeu dos Direitos Humanos condena a Espanha por duas "devoluções quentes" em Melilla*, <https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml>.

² Comissão Espanhola de Ajuda aos Refugiados (3 de outubro de 2017), *Tribunal Europeu dos Direitos do Homem condena Espanha por dois "regressos a quente"*, <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>.

³ Consejo General de la Abogacía Española (3 de outubro de 2017), *La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH*, <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>.

⁴ Dados do Eurostat, https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en.

as principais preocupações dos cidadãos do continente. Assim, o último "Eurobarómetro", publicado em novembro de 2024, destaca a imigração como a segunda prioridade em termos de áreas onde a UE deve atuar na opinião dos europeus, uma posição apoiada por 29% dos inquiridos (Comissão Europeia, 2024, p. 14), atrás apenas da Segurança e Defesa.

No entanto, embora a Comissão Europeia não hesite em responder a estas preocupações, apontando repetidamente para os "progressos" que estão a ser feitos na "gestão das fronteiras" (Comissão Europeia, 2022, p. 5), a verdade é que, quando se introduz na equação o fator da salvaguarda dos direitos fundamentais, a situação complica-se. Com efeito, as políticas de reforço do controlo fronteiriço, desenvolvidas com base nos objetivos de reforço do sistema em que assenta a segurança nacional e de garantia da soberania dos Estados, implicam medidas destinadas a dificultar a imigração ilegal que, pela sua própria natureza, afectam os direitos das populações em causa. E, de acordo com as regras básicas que regem o Estado de Direito, se essa incidência não for adequada, coerente e proporcional aos fins lícitos prosseguidos, pode representar uma intromissão ilegal no núcleo mais essencial dos direitos fundamentais, especialmente quando estes condicionam domínios fundamentais como o direito de asilo. O presente artigo de investigação pretende analisar este delicado equilíbrio, revelando os pontos de fricção entre as duas realidades antagónicas através de um exame detalhado da jurisprudência nacional e internacional; bem como esclarecer, na medida do possível, até onde pode ir a legalidade da atuação dos guardas civis na sua qualidade de guardas de fronteira.

2. ANÁLISE TEÓRICO-METODOLÓGICA: ESTADOS, FRONTEIRAS E PROTECÇÃO INTERNACIONAL

2.1. MAPA CONCEPTUAL DO AMBIENTE FRONTEIRIÇO

2.1.1 O conceito de fronteira

O termo "fronteira" tem quase tantos significados quantos os ramos da ciência que contemplaram o estudo de qualquer conceito derivado da noção intuitiva de "limite". Da matemática à ciência política, das relações internacionais ao direito. Sanz Donaire (2023, p. 254) afirma que o termo em questão provém do termo latino clássico *frons*, cujo significado remeteria para "frente" ou "fachada", e já ofereceria uma ideia do contexto antagónico ou distintivo em que se desenvolveria desde a sua formulação, fortemente ligada à esfera militar, à proteção contra o estrangeiro, o exterior. De facto, as fronteiras estão ligadas a conflitos e confrontos desde o Tratado de Mesilim, considerado o "tratado mais antigo de que há registo" (Doebbler, 2018, pp. 374-375), que mais não foi do que um acordo que regulava o reconhecimento dos limites entre vários reinos mesopotâmicos por volta de 2500 a.C. Também Curzon (1907) se expressou neste sentido nos primórdios do estudo científico das Relações Internacionais, ao afirmar que as tensões fronteiriças têm sido o fator mais importante nos conflitos entre Estados (p. 4).

Em todo o caso, é em tais antecedentes etimológicos que se baseiam as concepções actuais de fronteira, entre as quais se destaca, pela sua força discursiva, o Dicionário de Espanhol Jurídico, que afirma o seguinte

"Fronteira (Direito Internacional Público): *Linha que marca o limite exterior do território de um Estado, entendido como o espaço terrestre, marítimo e aéreo sobre o*

qual exerce a sua soberania, o que permite falar de fronteiras terrestres, marítimas e aéreas consoante a natureza física do espaço delimitado.

2.1.2 Fronteiras e soberania

De acordo com a tese de Lacan (1966), a compreensão dos conceitos assenta no entendimento das relações que estes desenvolvem relativamente às noções prévias que constituem o seu significado, através de uma concatenação de referências naquilo que o psicanalista francês conhecia como "cadeias de significantes" (pp. 501-502). Neste sentido, e tendo em conta a definição enunciada na epígrafe anterior, parece evidente que não podemos chegar a uma compreensão satisfatória da realidade em estudo sem antes estudarmos o outro conceito técnico que nela está em causa: o de soberania.

Muito se tem escrito sobre este conceito. Desde a primeira abordagem de John Bodin, no século XVI, em que as componentes nacional, territorial e teológica estavam intrinsecamente ligadas, a noção de soberania tem estado associada à existência de um vínculo que ultrapassa a mera extensão física e social em que o poder é exercido e que, de alguma forma, transcende o estritamente territorial. Talvez por isso não existam muitas fontes escritas de direito internacional que ofereçam uma definição cristalina e universal de soberania. Um dos poucos textos que nos pode dar alguma pista a este respeito é a Convenção de Montevideo sobre os Direitos e Deveres dos Estados, de 1933. Este tratado oferece o que, na prática, acabou por se tornar uma definição de soberania, ao estabelecer, no artigo 1.º, os requisitos básicos para que uma entidade estatal seja considerada um sujeito de direito internacional:

1. População permanente.
2. Território determinado.
3. Governo.
4. Capacidade de estabelecer relações com outros Estados.

É de salientar que, apesar de formalmente este tratado apenas ser aplicável ao reduzidíssimo número de Estados que o assinaram (foi acordado na Sétima Conferência Internacional Americana, antecessora direta da Organização dos Estados Americanos), "tem recebido uma adesão generalizada do ponto de vista doutrinário" (Infante Caffi, 2016, p. 66), estendendo-se gradualmente os seus postulados - quer por referência direta, quer por referência a um costume internacional neles apoiado - a uma generalidade de actores internacionais, incluindo a própria União Europeia. 66), estendendo gradualmente os seus postulados - quer por referência direta, quer por referência a um costume internacional neles baseado - a uma generalidade de actores internacionais, incluindo a própria União Europeia⁵.

⁵ Ver, por exemplo, as conclusões do Conselho Europeu sobre o processo de paz no Médio Oriente, de 20 de julho de 2015, ou a resolução do Parlamento Europeu sobre o papel da UE no processo de paz no Médio Oriente, de 10 de setembro de 2015; que promovem um caminho para o reconhecimento da Palestina como uma entidade política ("solução de dois Estados") com base numa população permanente (repetidamente referida como "população palestina"), um território permanente (assinalando o seu compromisso com as "fronteiras de 1967"), um governo efetivo (encarnado na "Autoridade Palestiniana", doravante ANP, que é expressamente citada) e uma capacidade de estabelecer relações com outros Estados (citando e reconhecendo os acordos alcançados com a referida ANP).

De igual modo, a jurisprudência internacional foi definindo progressivamente o conceito de soberania, sendo que, na ausência de um título objetivo (por exemplo, um tratado de limites assinado e respeitado por todos os Estados envolvidos), um Estado é considerado soberano sobre um território quando manifesta a sua intenção de o ser através de meios adequados para o efeito no direito internacional (por exemplo, uma declaração unilateral) e, ao mesmo tempo, quando esse Estado é capaz de exercer essa autoridade de forma prática, através do desenvolvimento efetivo da jurisdição sobre o território (Acórdão do Tribunal Permanente de Justiça Internacional de 19 de abril de 1955), uma declaração unilateral) e, ao mesmo tempo, quando esse Estado é capaz de exercer essa autoridade de forma prática, através do desenvolvimento efetivo da jurisdição sobre o território (Acórdão do Tribunal Permanente de Justiça Internacional de 5 de abril de 1933, pp. 45-27 in fine, 46-28 in limine; Acórdão do Tribunal Internacional de Justiça de 17 de dezembro de 2002, n.º 134, pp. 182-61; Sentença do Tribunal Permanente de Arbitragem de 9 de outubro de 1998, n.º 239, p. 268; entre outros).

Será com base nesta soberania que se fundará o direito legítimo dos Estados de protegerem as suas fronteiras, habitualmente protegido pelas regras tradicionais do direito internacional consuetudinário e pela referência ao artigo 51º da Carta das Nações Unidas; e, no caso europeu, transcenderá o nível nacional, tendo em conta a obrigação internacional que o Acordo de Schengen implica para os seus signatários.

2.2. MIGRAÇÃO E ASILO

Por outro lado, quando se trata de conceitos relacionados com os direitos dos indivíduos que se encontram na zona fronteiriça, não é raro surgirem alguns mal-entendidos (por exemplo, no que diz respeito às noções de "imigrante" e "refugiado"), o que torna aconselhável um estudo breve mas rigoroso deste ambiente jurídico, especialmente no que diz respeito ao conteúdo e ao âmbito da proteção internacional.

2.2.1 Direito de asilo e proteção subsidiária

O termo "asilo" provém do grego *asylon*, palavra cuja tradução se aproxima da de "lugar inviolável". Na sua conceção inicial, era a condição que se atribuía ao *hieron*, uma espécie de espaço especial localizado no interior dos *témenos*, áreas consagradas aos deuses (Harris Díez, 2011, p. 70), que estavam fora da jurisdição do Estado, "podendo assim tornar-se um refúgio para indivíduos perseguidos, escravos fugidos ou políticos" (Zaidman e Schmitt-Pantel, 2002, p. 45). Foi neste contexto que se formou o dogma cristão do "asilo no sagrado", um estatuto de imunidade tradicionalmente conferido aos locais de culto para proteger os necessitados e redimir os criminosos arrependidos (Golmayo, 1866, pp. 88-89), do qual derivaria, por sua vez, o conceito moderno de "direito de asilo".

Este conceito moderno de direito de asilo será estabelecido fundamentalmente através da proclamação de dois textos: a Convenção de Genebra de 1951 relativa ao Estatuto dos Refugiados (a seguir denominada Convenção de Genebra), que estabelece o conceito de refúgio, e o seu Protocolo de 1967, que generaliza esta proteção, inicialmente criada para um grupo muito limitado de beneficiários. A combinação destes dois textos permite chegar a uma definição única que reconhece como refugiado ou beneficiário de asilo qualquer pessoa que

"...devido a um receio fundado de ser perseguido em virtude da sua raça, religião, nacionalidade, pertença a um determinado grupo social ou opiniões políticas, se encontre fora do país de que é nacional e não possa ou, em virtude desse receio, não queira pedir a proteção desse país; ou, se se encontrar numa situação irrazoável fora do país onde tinha a sua residência habitual, não possa ou, em virtude desse receio, não queira regressar a esse país".

Por outro lado, embora esta seja a definição geral, o facto é que os diferentes modelos de proteção dos direitos fundamentais existentes desenvolveram todo um conjunto de normas que ampliam e clarificam o conteúdo deste direito. Na União Europeia, este trabalho é feito através da Diretiva 2011/95/UE, que estabelece aspectos nucleares no âmbito do processo de obtenção do estatuto de refugiado, como os critérios de apreciação das circunstâncias que podem ser consideradas como perseguição, ao mesmo tempo que (e isto é extremamente relevante) introduz no direito comunitário a chamada "proteção subsidiária", garantia que salvaguarda a situação jurídica dos nacionais de países terceiros e apátridas que, "não preenchendo os requisitos de asilo, [...] existam motivos sérios para crer que se encontram em situação de perseguição", e que "não preenchendo as condições para obter asilo, [...] existam motivos sérios para crer que se encontram em situação de perseguição". existem motivos sérios para crer que, se regressassem ao seu país de origem [...] correriam um risco real" (art. 4). Esta proteção subsidiária - que, juntamente com o direito de asilo, constitui o que, na terminologia da UE, se designa genericamente por "proteção internacional" - destina-se a alargar a indemnização do estatuto de refugiado às pessoas que correm o risco de serem condenadas à morte, sujeitas a tortura ou mesmo de sofrerem as consequências da guerra.

Em todo o caso, todos os regulamentos acima referidos estabelecem explicitamente a inaplicabilidade desta proteção às pessoas que possam ser consideradas autores de crimes internacionais graves (criminosos de guerra, genocidas, etc.), fugitivos de crimes comuns graves ou pessoas que representem um perigo para a segurança do país de acolhimento.

2.2.2 Direitos aplicáveis aos beneficiários de proteção internacional

Toda a proteção internacional confere uma série de direitos mínimos aos seus beneficiários, embora alguns aspectos acidentais destes (prazos, prorrogação, etc.) possam variar ligeiramente consoante o estatuto concedido seja o de asilo (mais protegido) ou o de proteção subsidiária (menos protegido). Além disso, uma parte importante destes direitos será também exercida não só por aqueles que foram oficialmente reconhecidos como beneficiários de qualquer tipo de proteção, mas a regulamentação europeia reconhece também a sua aplicabilidade a simples requerentes, desde que o seu caso não tenha sido resolvido⁶. Em qualquer caso, existem dois direitos fundamentais que estão intrinsecamente ligados a qualquer forma de proteção internacional - incluindo os requerentes - e cuja natureza será decisiva no conflito entre os direitos individuais e a segurança nacional: a proteção judicial efectiva e a não repulsão.

⁶ Por exemplo, e em conformidade com as disposições da Diretiva 2013/33/UE, o direito de acesso aos cuidados de saúde (art. 19.º), aos apoios públicos (art. 18.º) ou ao mercado de trabalho (art. 15.º).

2.2.2.1 O direito a uma proteção judicial efectiva

O direito a uma tutela judicial efectiva, entendido como a garantia de que os cidadãos têm "acesso à jurisdição, à tramitação do processo, à resolução [razoável] do caso e à execução da sentença" (Carrasco Durán, 2020, p. 20), no quadro de um sistema judicial justo e imparcial, não é uma garantia específica do direito de asilo, mas o seu alcance é universal e, como tal, está consagrado na Constituição espanhola (art. 24.º) e na Constituição espanhola (art. 20) no quadro de um sistema judicial justo e imparcial, não é uma garantia específica do direito de asilo, mas o seu âmbito é universal e, como tal, está incluído na Constituição espanhola (art. 24.º) e na Carta dos Direitos Fundamentais da UE (art. 47º), sob a referência permanente aos direitos a um julgamento justo (art. 6º) e a um recurso efetivo (art. 13º).

No entanto, o seu impacto na área do direito de asilo tem sido notável, ao ponto de a Diretiva 2013/32/UE garantir (art. 46.º) o acesso ao recurso nos procedimentos de asilo, afirmando explicitamente que este deve ser apreciado por um órgão "judicial". Assim, uma das alegações mais recorrentes na contestação da atuação do Estado na zona de fronteira tem sido a alegada falta ou precariedade de acesso aos recursos judiciais. Neste sentido, e no âmbito europeu, a garantia jurisdicional última de uma tutela jurisdicional efectiva tem sido canalizada - antes do esgotamento das instâncias nacionais - através do recurso ao TEDH por violação do artigo 13.º da CEDH⁷. No entanto, a jurisprudência deste tribunal é clara: para se constatar uma violação do artigo 13º, deve existir primeiro uma alegação plausível de violação de qualquer outro dos direitos garantidos pela Convenção. Embora não seja necessário que tal violação tenha efetivamente ocorrido, tem sido exigido que exista uma *queixa plausível* ao abrigo da Convenção - acórdão da CEDH (Grande Secção) de 23 de fevereiro de 2012, *Hirsi Jamaa v. Itália*, §197, que, a partir de uma primeira aproximação plausível, permita depois compor um relato fiável dos factos, dado que a Convenção se destina a garantir direitos práticos e efectivos, e não teóricos ou ilusórios - CEDH (Grande Secção) Acórdão de 13 de fevereiro de 2020, *Caso N. T. e N. D. v. Espanha*, §171-. É, pois, raro encontrar violações isoladas do artigo 13.º em que não se verifique qualquer outra violação, embora doutrinariamente a possibilidade exista, e de facto tenha ocorrido - CEDH (Grande Secção), Acórdão de 8 de julho de 2003, *Hatton e Outros v. Reino Unido*. No domínio do direito de asilo, esta relação tem sido quase invariavelmente transmitida através da ligação da infração com violações do artigo 3.º da CEDH⁸ e do artigo 4.º do Protocolo n.º 4 da CEDH.⁹

2.2.2.2 Direito de não repulsão

Por seu turno, o direito à não repulsão (consagrado no artigo 33.º da Convenção de Genebra e habitualmente designado por *non-refoulement* na doutrina internacional) é um princípio básico da proteção internacional que implica a garantia de que o beneficiário de proteção não será devolvido ao seu Estado de origem ou a qualquer outro onde corra o risco de ser perseguido, enquanto mantiver o seu estatuto. Este direito estende-se diretamente aos requerentes durante a apreciação do seu caso e, a nível da UE, mesmo àqueles

⁷ "Toda a pessoa cujos direitos e liberdades consagrados na presente Convenção tenham sido violados deve ter um recurso efetivo perante uma autoridade nacional, mesmo que a violação tenha sido cometida por pessoas que actuem no exercício de funções oficiais.

⁸ "Ninguém pode ser submetido a tortura, nem a penas ou tratamentos desumanos ou degradantes".

⁹ "São proibidas as expulsões colectivas de estrangeiros".

cuja proteção internacional não tenha sido oficialmente concedida ou tenha sido retirada (art. 14.º, n.º 6, da Diretiva 2011/95/UE), na medida em que "são as circunstâncias de facto de uma pessoa, [e] não a validação oficial dessas circunstâncias, que dão origem ao estatuto de refugiado da Convenção" (Hathaway, 1995, 303-304). E, ao mesmo tempo, a sua observância é independente do facto de o requerente se encontrar ou não em situação regular no país, facto que - apesar de não constar expressamente dos artigos da Convenção - se impõe por via do direito internacional consuetudinário e, no caso europeu, foi consagrado pelo artigo 19.º da CDFUE e pelo artigo 9.º da Diretiva 2013/32/UE, sendo referendado através de uma jurisprudência reiterada e pacífica a este respeito no quadro do sistema europeu de proteção dos direitos humanos¹⁰. Isto significa que o direito ao non-refoulement se configurou como parte do núcleo mais essencial dos direitos dos refugiados, na lógica de que a sua violação sistemática significaria, na prática, o esvaziamento do conteúdo da proteção internacional.

É de salientar que este princípio admite uma exceção: o artigo 33.2 da Convenção de Genebra garante a sua inaplicabilidade nos casos em que existem "razões sérias" para considerar que o beneficiário ou requerente de proteção internacional pode ser considerado "um perigo para a segurança do país onde se encontra" (art. 33.2). Esta disposição, que reforça as prerrogativas dos Estados no âmbito do seu direito legítimo de proteger as suas fronteiras, foi aprovada, com algumas nuances¹¹, pela jurisprudência internacional. Um bom exemplo é o acórdão do TEDH (Grande Secção) de 29 de abril de 1997, *L.H.R. v. França, no caso L.H.R. v. França*. O Tribunal de Justiça aprovou a expulsão de um cidadão colombiano, condenado por tráfico de droga, para o seu país de origem, com o fundamento de que a sua presença constituía uma "grave ameaça para a ordem pública", apesar das advertências do requerente - partilhadas pela extinta Comissão Europeia dos Direitos do Homem, e mesmo tibiamente pelo próprio Tribunal - de que a conclusão da sua expulsão poderia constituir um perigo para a sua vida.

Por fim, uma última questão digna de nota é a de que o desenvolvimento do princípio do non-refoulement deu lugar, ao longo do tempo, ao aparecimento de um princípio complementar que tem sido geralmente retomado pelos mais importantes instrumentos jurídicos internacionais sobre a matéria: a proibição de expulsões colectivas de estrangeiros. Este preceito, que alguns autores como Kamto (2007) consideram (não sem controversia) como um "princípio geral de direito internacional" (p. 129), foi normativizado na CEDH (artigo 4.º do Protocolo n.º 4) e na CDFUE (artigo 19.º, n.º 1). O seu conteúdo refere-se à abordagem segundo a qual qualquer expulsão de estrangeiros deve basear-se em circunstâncias não arbitrárias, exigindo assim uma avaliação individual do contexto de cada estrangeiro.

¹⁰ Acórdãos do TEDH de 7 de julho de 1989, *Soering contra o Reino Unido* e, em especial, de 15 de novembro de 1996, *Chahal contra o Reino Unido*.

¹¹ Por exemplo, a aplicação deste preceito a nível europeu não deve significar que, por omissão, conduza à violação do artigo 3º da CEDH, que proscreve a tortura e as penas ou tratamentos desumanos ou degradantes; Um fator que, por outro lado, é aplicável a toda a comunidade internacional, tendo sido considerado um argumento de natureza *jus cogens* (Acórdão do Tribunal Penal Internacional para a ex-Jugoslávia de 22 de fevereiro de 2001, *Procurador v. Dragoljub Kunarac Radomir Kovac And Zoran Vukovic*, §466; ou Acórdão do Tribunal Internacional de Justiça de 20 de julho de 2012, Questões relativas à obrigação de perseguir ou extraditar, *Bélgica v. Senegal*, §99).

3. ANÁLISE JURÍDICA: POSIÇÕES ANTAGÓNICAS E RESPOSTA DO TRIBUNAL

3.1. *HIRSI JAMAA V. ITÁLIA*: A GÉNESE DE UMA DOUTRINA

Com base na referida legislação, os sucessivos pronunciamentos judiciais têm vindo a delinear gradualmente o quadro normativo final que, pelo menos por enquanto, rege o complicado equilíbrio entre os poderes legítimos do Estado e a salvaguarda dos direitos fundamentais. Para o efeito, destaca-se um acórdão que, devido ao período de tempo em que foi proferido e às suas implicações políticas subsequentes, se tornou uma referência incontornável para o estabelecimento dos critérios mínimos de atuação na fronteira: o Acórdão (Grande Secção) do TEDH de 23 de fevereiro de 2012, *Hirsi Jamaa et al. contra Itália*.

Hirsi Jamaa é o nome de um cidadão somali que fazia parte de um grupo de cerca de 200 imigrantes ilegais desembarcados no porto de Trípoli entre 6 e 7 de maio de 2009. Este desembarque foi efectuado diretamente a partir das três embarcações do Estado italiano (*Guardia di Finanza* e Guarda Costeira) que tinham procedido, algumas horas antes, à interceção e ao salvamento do grupo quando este navegava em embarcações precárias, cerca de 35 milhas náuticas a sul da ilha de Lampedusa, na zona de busca e salvamento maltesa (a seguir designada SAR). Na sequência destes factos, a Itália foi processada perante o TEDH, tendo-se juntado ao processo um total de vinte e cinco partes.

No entanto, o que foi relevante - pela sua novidade - em *Hirsi Jamaa* não foi tanto a aplicação do artigo 3.º da CEDH no contexto de um retorno de imigrantes - prática já consolidada em acórdãos como *Chahal v. Reino Unido* - mas sim o facto de, pela primeira vez, o tribunal ter tido a oportunidade de se pronunciar sobre a rejeição de imigrantes interceptados em ambiente marítimo ao mesmo tempo que avaliava a aplicação extraterritorial da CEDH (Alarcón Velasco, 2015, p. 4). E fê-lo desferindo um rude golpe na tese italiana, ao declarar a violação dos artigos 3º e 13º da CEDH, bem como do artigo 4º do seu protocolo nº 4, em todos os casos por unanimidade.

O raciocínio central subjacente à posição do tribunal foi o seguinte:

1. A nível geral, a CEDH é aplicável na medida em que, em conformidade com os artigos 92º e 94º da Convenção das Nações Unidas sobre o Direito do Mar, os navios em que ocorreram os factos estão sujeitos à jurisdição do seu Estado de bandeira, tratando-se de um caso de "exercício extraterritorial de jurisdição [...] suscetível de implicar a responsabilidade do Estado".
2. No que diz respeito ao artigo 3.º, o fator determinante foi a impossibilidade de considerar a Líbia como um "*lugar seguro*" para o desembarque, uma vez que o tribunal considerou que não só a segurança do ponto de vista marítimo deve ser tida em conta¹², mas também questões relacionadas com a proteção dos seus direitos fundamentais (violação do princípio da não repulsão).

¹² A ausência de risco nos conceitos relacionados com a segurança no mar que se encontram nas convenções internacionais sobre a matéria (em especial nas convenções SAR e SOLAS) remete, na sua maioria, por referência, para aspectos relacionados com a segurança da navegação ou operacional (*safety*, segurança como proteção contra o naufrágio, contra o afogamento, contra os riscos inerentes à carga do navio, etc.). Não obstante o exposto, e em relação ao conceito de "*local de segurança*" existente na Convenção SAR de

3. No que diz respeito ao artigo 4.º do Protocolo n.º 4, o fator determinante foi a falta de individualização da expulsão dos imigrantes, na medida em que não foram identificados e não se avaliou se algum deles poderia ter circunstâncias pessoais relevantes (violação da proibição de expulsões colectivas).

4. No que diz respeito ao artigo 13.º, o fator determinante foi a impossibilidade de os imigrantes terem acesso a um recurso efetivo contra a decisão de expulsão (violação do direito à proteção judicial efectiva), fator que pode ser avaliado tendo em conta a violação do artigo 3.

3.2. CASO *N.D. e N.T. v. ESPANHA*: OS LIMITES DA PROTECÇÃO

Tal como referido nas secções anteriores, a universalidade do direito de procurar proteção internacional não implica que esse direito possa ser reivindicado ou exercido de forma ilimitada. O Acórdão do TEDH (Grande Secção) de 13 de fevereiro de 2020, no âmbito do caso *N. D. e N. T. v. Espanha*, será apenas um dos melhores exemplos de como as nações podem, por si só, estabelecer esquemas eficientes de controlo de fronteiras que, por sua vez, respeitem o direito internacional humanitário, combatendo o abuso de direitos numa perspetiva garantística.

Emulando a análise efectuada na secção anterior relativamente a *Hirsi Jamaa*, o presente caso envolve dois cidadãos estrangeiros, N. D. e N. T., que, como parte de um grupo de cerca de 600 pessoas, tentaram invadir a vedação da fronteira na cidade de Melilla na madrugada de 13 de agosto de 2014. A sua tentativa foi frustrada graças à ação da Guardia Civil e das forças de segurança marroquinas, tendo os dois queixosos sido escoltados para o outro lado da fronteira, um ato que motivará a ação judicial. Posteriormente, ambos os actores participariam em dois novos assaltos à vedação, conseguindo aceder ilegalmente ao território espanhol. É relevante que um deles viesse mais tarde a solicitar proteção internacional, embora esta tenha sido negada em todas as instâncias processuais.

Nesta altura, o interesse do acórdão é duplo. Por um lado, porque foi o aval definitivo à prática do "*rechaço na fronteira*" (por vezes designado pejorativamente por "*retorno a quente*"): a execução de um retorno imediato a Marrocos de qualquer imigrante apanhado a tentar ultrapassar ilegalmente os elementos de contenção da fronteira. E, por outro lado, porque representa um contraponto à *Hirsi Jamaa*, uma vez que ambas marcam os limites da legalidade numa perspetiva diferente: positiva na *N. D.* e na *N. T.* (o que se pode fazer), negativa na *Hirsi Jamaa* (o que não se pode fazer), indicando assim os dois limites entre os quais a legislação fronteiriça deve circular. Tudo isto no contexto da existência, neste caso, de uma decisão de primeira instância que contradizia os argumentos de Espanha, o que deu origem a um processo de fundamentação mais pormenorizado por parte da Grande Secção em resposta às alegações dos queixosos, que contestavam a atuação dos guardas de fronteira por violação do artigo 3.º da CEDH e do artigo 4.º do Protocolo n.º 4 da CEDH, bem como do artigo 13.

Assim, o raciocínio central subjacente à posição do tribunal foi o seguinte:

1979, a própria Organização Marítima Internacional (doravante IMO) acabou por integrar nuances que complementam esta visão, resultando em textos como o Anexo 34 da Resolução MSC.167(78) da IMO, *Guidelines on the treatment of persons rescued at sea*, em que se faz referência a regulamentos como a Convenção de Genebra de 1951.

1. No que respeita ao artigo 3.º, já na mesma fase de admissão (decisão de 7 de julho de 2015), o Tribunal rejeita liminarmente a admissibilidade dos argumentos dos queixosos quanto à possibilidade de o princípio de não repulsão (artigo 3.º da CEDH) ter sido violado pela recusa de regresso dos imigrantes a Marrocos. Embora o raciocínio jurídico não seja particularmente detalhado, destaca claramente a ausência de provas para considerar Marrocos um lugar inseguro para tais fins, e nem mesmo - como fez no caso de *Hirsi Jamaa* - considera necessário considerar a questão em maior profundidade.
2. No que diz respeito ao artigo 4.º do Protocolo n.º 4, a posição do Tribunal é que não se pode considerar que exista uma expulsão colectiva no contexto de uma ação em vigor desencadeada pelo próprio requerente e que provoca "uma situação claramente perturbadora, difícil de controlar e que põe em perigo a segurança pública" (§201). Isto é particularmente relevante se tivermos em conta que, no acórdão do tribunal de primeira instância, a Câmara tinha estabelecido diretamente - sem sequer levantar uma justificação que afectasse o mérito do caso - um paralelismo total deste caso com o de *Hirsi Jamaa*, apesar de serem contextos totalmente diferentes. Assim, o tribunal prevê que o "exame individualizado" que permite ultrapassar o obstáculo concetual da expulsão colectiva deve ser efectuado tendo em conta "as circunstâncias particulares da expulsão e o 'contexto geral no momento dos factos'" (§197), o que, por sua vez, permite simplificar ou omitir os procedimentos de avaliação, especialmente se este contexto depender em grande medida "do comportamento do próprio requerente" (§200) e se o Estado fornecer "procedimentos legais disponíveis para entrar [no país]" (§208) e "garantir o direito de procurar proteção [...] de forma real e efectiva" (§208) e "o direito de procurar proteção [...] for garantido [...]" (§209).de uma forma real e efectiva" (§208).
3. No que diz respeito ao artigo 13.º, o Tribunal esclarece que não se verifica qualquer violação do direito a uma proteção jurisdicional efectiva, atribuindo igualmente a falta de recurso jurisdicional à "própria conduta dos requerentes ao tentarem entrar em Melilla sem autorização" (§242).

Por último, uma observação interessante sobre a fundamentação do acórdão é que, embora o Tribunal rejeite a tese espanhola relativa à limitação da competência com base em critérios operacionais - semelhantes aos defendidos pela Itália no processo *Hirsi Jamaa*-, afirmando que o exercício efetivo da autoridade que a Espanha, através da Guardia Civil, exerce a partir do perímetro da vedação exterior para o interior (§§107-108), é inegável, estabelece que o Governo espanhol não pode ser responsabilizado por circunstâncias ocorridas fora do seu território soberano, O facto de o Governo espanhol, através da Guardia Civil, exercer a sua ação do perímetro da vedação exterior para o interior (§§107-108), estabelece que o Governo espanhol não pode ser responsabilizado por circunstâncias que ocorram fora do seu território soberano e, em particular, por aquelas que sejam levadas a cabo por agentes de um Estado terceiro (§218).

3.3. ANÁLISE COMPARATIVA: A COMPATIBILIDADE DE UMA DOUTRINA JURISPRUDENCIAL DÍSPAR

Como vimos, tanto *Hirsi Jamaa e outros v. Itália* como *N.D. e N.T. v. Espanha* representam dois casos em que, para condutas a priori análogas (a entrega a autoridades não europeias de estrangeiros que tentam entrar ilegalmente em território comunitário), o TEDH proferiu decisões diferentes. E isto deve-se fundamentalmente à existência no caso *N.D. e N.T.* de um fio condutor que foi devida e oportunamente invocado pela Espanha no âmbito dos procedimentos seguidos durante o referido contencioso, e que articula, do princípio ao fim, o acórdão: a doutrina do "comportamento culposos".

O corolário deste raciocínio é que o Estado não pode ser responsabilizado pelo facto de os imigrantes se furtarem aos procedimentos legais para entrarem no país, especialmente se "aproveitarem deliberadamente o seu grande número e usarem a força" (*N.D. e N.T. v. Espanha*, §201). Assim, para que esta doutrina seja aplicável, o comportamento censurável imputável aos imigrantes deve gerar uma situação grave, decorrente de uma conduta dolosa - ou seja, consciente da sua ilegalidade e das suas possíveis consequências - que represente um perigo objetivo para a segurança pública, incluindo a dos próprios imigrantes.

Com efeito, a interpretação do Tribunal transcende todas as alegadas violações invocadas pelos requerentes, mesmo aquelas que (a priori) estão mais afastadas da sua esfera de ação individual. Assim, no que diz respeito à proibição de expulsões colectivas de estrangeiros (artigo 4.º do Protocolo n.º 4 da CEDH), o TEDH situará o aspeto diferencial nas possibilidades de acesso dos imigrantes aos procedimentos legais de entrada no território europeu. Assim, em *N. D. e N. T.*, afirma-se repetidamente que a legislação espanhola oferecia várias possibilidades aos requerentes de processarem a sua entrada em Espanha, bem como de solicitarem asilo¹³ (§212), mas que estes instrumentos foram recusados (conduta culposa) pelos requerentes (§231). O mesmo raciocínio se aplica ao direito à proteção judicial efectiva (artigo 13.º da CEDH), uma vez que os argumentos utilizados pelo Tribunal de Garantias são os mesmos (§242).

Uma vez expostas estas premissas, coloca-se inevitavelmente a questão: poderá a doutrina do comportamento culposos ser utilizada, *mutatis mutandis*, para as expulsões que têm lugar no domínio marítimo? E, em caso afirmativo, o que seria necessário alterar no quadro da ação do Estado para o fazer? A resposta a estas questões não é trivial. Na sequência de *N.D. e N.T.*, o TEDH recorreu a esta doutrina - que, de resto, não era inteiramente nova aquando da sua formulação¹⁴ - em algumas ocasiões¹⁵, embora nenhuma

¹³ A possibilidade oferecida pela legislação espanhola de aceder a certos procedimentos relacionados com o asilo em embaixadas e consulados (artigo 38.º da Lei 12/2009, de 30 de outubro, que regula o direito de asilo e a proteção subsidiária) é particularmente digna de nota, tanto devido à ênfase repetida pelo Tribunal de Justiça nesta possibilidade, como porque não é uma prática comum noutros Estados europeus (a Itália, por exemplo, não a inclui no seu Decreto Legislativo de 19 de novembro de 2007, sobre o reconhecimento da proteção internacional).

¹⁴ O TEDH já tinha utilizado uma abordagem precursora em 1996, no caso *John Murray v. Reino Unido* - Acórdão (Grande Secção) de 8 de fevereiro de 1996 - quando recusou proteção a um homem condenado por terrorismo que alegava que o seu silêncio tinha sido utilizado contra ele no contexto do seu processo judicial. O tribunal considerou que foi ele que optou por permanecer em silêncio, apesar de estar consciente das consequências que tal comportamento poderia acarretar, e que, por conseguinte, foi ele que se expôs à inferência de que o seu silêncio o prejudicava (§56).

¹⁵ Acórdão do TEDH (Terceira Secção) de 24 de março de 2020, *Asady e outros v. Eslováquia*.

delas tenha servido para endossar uma recusa marítima. No entanto, o que é certo é que não há nenhuma passagem em *N.D. e N.T.* em que o tribunal afirme que a sua doutrina não é válida para expulsões de imigrantes interceptados no mar. Muito pelo contrário: o acórdão sublinha a necessidade de uma avaliação das "circunstâncias do caso concreto" (§201). Por conseguinte, e de acordo com o princípio *permissum videtur id omne quod non prohibetur*¹⁶, parece lógico deduzir que a admissibilidade de tal princípio deve depender apenas do cumprimento dos seus pressupostos intrínsecos, ou seja, da existência de instrumentos jurídicos efectivos que permitam o acesso ao Estado de destino e o início de um procedimento de asilo junto das suas autoridades; bem como na constatação de um comportamento censurável por parte dos imigrantes que, ignorando a existência de tais instrumentos jurídicos, desafiam os mecanismos de controlo fronteiriço através de acções coercivas. Além disso, ambos os pressupostos devem ser devidamente invocados pelo Estado no processo judicial, o que a Itália não fez no caso *Hirsi Jamaa*. Nenhum destes pressupostos parece necessariamente invencível num cenário marítimo típico em que centenas de homens de origem e antecedentes desconhecidos se colocam a si próprios, aos seus companheiros de viagem e aos guardas fronteiriços e costeiros europeus em perigo manifesto ao proporem uma partida maciça, planeada e coordenada de embarcações com destino a um território isolado, com capacidades de acolhimento limitadas, com o consequente risco de colapso - como Lampedusa. Tudo isto está sujeito à necessidade de o Estado costeiro dispor de um dispositivo diplomático adequadamente dimensionado, com poderes concedidos no domínio do asilo, que lhe permita justificar a suficiência dos mecanismos de acesso ao asilo. A este propósito, refira-se ainda a comunidade que a UE representa em matéria de migrações e asilo, o que permitiria mesmo sugerir - embora talvez para isso fosse necessário avançar mais no sempre lento processo de integração europeia - que a existência de delegações diplomáticas de outros países da UE é um ativo que deve necessariamente ser valorizado para efeitos de adequada ponderação das possibilidades de acesso oferecidas pelo Estado litigante, pois representa um inerente reforço dos recursos próprios do Estado.¹⁷

E, em consonância com o exposto, é também pertinente trazer à colação algumas inferências relativas à problemática das limitações factuais do Estado na sua ação internacional. Apesar de certos autores, como Sánchez Tomás (2018, p. 110) ou Martínez Escamilla (2021, pp. 6-7), reivindicarem a territorialidade como a perspetiva dominante em termos de determinação da responsabilidade internacional, a verdade é que tanto a doutrina como a prática internacionais (já referidas no ponto 2.1.2 do presente texto) apontam para a necessidade de um exercício prático da territorialidade na determinação da responsabilidade internacional.² do presente texto) apontam para a necessidade de um exercício prático de autoridade nesse território para que este possa ser considerado soberano, razão pela qual o tribunal, no seu acórdão da Grande Secção, altera a sua decisão de primeira instância, eliminando ou atenuando fortemente as menções relativas à preponderância do traçado da fronteira em detrimento do traçado efetivo da vedação (incluídas

¹⁶ "Tudo o que não é proibido é considerado permitido".

¹⁷ Afinal, parece óbvio pensar que, dada a preexistência de um espaço comum de liberdade, segurança e justiça, no âmbito do qual foram abolidas as fronteiras internas e que articulou mecanismos de implementação de uma política comum de imigração e asilo, uma rede constituída por todas e cada uma das suas embaixadas e consulados proporciona aos candidatos à imigração uma plataforma de acesso muito maior, mais diversificada e com um maior número de garantias processuais do que a oferecida por um Estado isolado. Sobretudo se tivermos em conta a homogeneidade que a legislação europeia implica no que diz respeito ao reconhecimento, qualificação, avaliação e resolução dos procedimentos de asilo, permanência e residência legal, que são comuns a todos os seus Estados membros.

no §53 do acórdão de primeira instância). Assim, como já referimos, a rejeição da isenção do princípio geral de atribuição não depende da territorialidade do ponto onde os actos têm lugar, mas do facto de a ação ser levada a cabo por agentes do Estado signatário, independentemente do local onde a ação tem lugar. Este aspeto será relevante nos casos (por exemplo, os acontecimentos de 24 de junho de 2022 em Melilla) em que a Espanha foi considerada responsável por actos praticados por funcionários estrangeiros em zonas que, embora formalmente dentro da fronteira "histórica" espanhola, na prática se situam para além da vedação, não sendo, por conseguinte, objeto de qualquer controlo efetivo por parte da Espanha.

Por fim, é de salientar a diferença de tratamento que o tribunal dá ao estudo de eventuais violações do artigo 3.º da CEDH (prevenção da tortura e de tratamentos desumanos ou degradantes) em *Hirsi Jamaa* e em *N.D. e N.T.* Apesar da escassa justificação oferecida pela decisão de inadmissibilidade de *N.D. e N.T.* a este respeito, parece claro que a justificação para esta diferença reside, pelo menos em grande parte, no país de expulsão. Uma parte da doutrina (Del Valle Gálvez, 2018, pp. 25-49; Freedman, 2024, 204-220) tem vindo a apresentar teses que se aproximam de um questionamento generalizado do que se passou a designar por "políticas de externalização de fronteiras", conceito com o qual é necessário ter muita cautela. Em primeiro lugar, porque este termo pejorativo tem sido utilizado para definir o que, na maior parte dos casos, não passa de políticas de cooperação policial internacional em matéria de controlo de fronteiras, através das quais se promove o reforço das capacidades de aplicação da lei nos países em desenvolvimento. Assim, até o próprio termo escolhido parece bastante infeliz, uma vez que é difícil "externalizar" as tarefas de controlo fronteiriço e de aplicação da lei, que não são mais do que "obrigações derivadas tanto do direito convencional como do direito consuetudinário" e, portanto, objeto de "*ius cogens*" (Soler García, 2017, p. 41). E, por outro lado, porque a aceitação irracional de posições tangencialmente contrárias a essas políticas poria em causa não só a aplicação de medidas legítimas do Estado - expressão da sua soberania em matéria de segurança nacional ou de política migratória -, mas também os interesses da comunidade internacional e a proteção dos direitos humanos: afinal, a capacitação dos Estados de origem e de trânsito em matérias vitais como a busca e salvamento no mar dos seus próprios compatriotas é também parte essencial dessa cooperação. Por conseguinte, esta cooperação não pode, *por si só, estar em* contradição com a CEDH.

E é aqui que entra o verdadeiro fator diferencial de *Hirsi Jamaa*: a Líbia. Neste sentido, a situação da Líbia é certamente idiossincrática. Trata-se de um Estado que não assinou a Convenção de Genebra, que foi repetidamente definido por diferentes autores como um "caos", no qual "os migrantes expulsos da Europa eram frequentemente deixados a um destino incerto" (Cole, 2012, p. 6). E isto explica perfeitamente os receios expressos pelo tribunal no processo *Hirsi Jamaa* (§136), com base em vários relatórios incorporados no processo (ACNUR, Comissão Europeia, Conselho da Europa, Human Rights Watch, etc., ver §33-42). Esta situação não é comparável à existente em praticamente todos os Estados com os quais a Espanha tem acordos de repatriamento activos e razoavelmente funcionais, principalmente Marrocos e Argélia, Estados que fazem parte da Política Europeia de Vizinhança - que exige, de acordo com o artigo 8.º do TUE, a partilha dos princípios democráticos da UE - e que dela beneficiaram muito, tornando-se

parceiros económicos e políticos privilegiados. Afinal, existe uma abundância de pronunciamentos judiciais¹⁸ que endossam explicitamente o seu estatuto de "países terceiros seguros" (ver SAN 1441/2018 de 15 de março de 2018 para o caso de Marrocos ou SAN 3838/2016 de 17 de outubro de 2016 para o caso da Argélia). Trata-se de um ponto de grande interesse, não só para efeitos de regresso dos migrantes em situação irregular aos seus países de origem, mas também no que diz respeito à possibilidade (consagrada no artigo 3.º, n.º 3, do Regulamento n.º 604/2013 relativo à determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional) de encaminhar os requerentes de asilo para centros situados em países terceiros seguros durante o exame do seu pedido. No entanto, esta possibilidade poderia ser objeto - dada a sua complexidade e previsível controvérsia - de um artigo separado, com o correspondente debate doutrinal.

4. CONCLUSÕES

Para concluir, faremos uma breve síntese da doutrina revista nos capítulos anteriores, oferecendo algumas linhas de orientação que descrevem os resultados de maior interesse na matéria em análise.

Em primeiro lugar, a conclusão mais geral e óbvia que se pode extrair do exposto é que no ambiente fronteiriço convergem numerosos fenómenos sociais que geram um elevado nível de litigiosidade em matéria de proteção dos direitos fundamentais. Estes processos, todos eles derivados da permanente tensão entre as políticas de controlo migratório e as garantias individuais, exigem um equilíbrio que muitas vezes é resolvido nos tribunais, pondo à prova os quadros jurídicos nacionais e internacionais; bem como uma série de conceitos tratados pela doutrina - fronteira, soberania, território, asilo, etc. - que, apesar de habitualmente utilizados de forma trivial, possuem um conteúdo de grande força jurídica, política, social e até histórica. É, pois, fundamental que as forças de segurança que prestam serviço nas fronteiras tenham conhecimento suficiente da legislação que as protege, de modo a desempenharem as suas funções com eficiência, mas também com respeito pelos direitos daqueles que passam por esses ambientes.

Por outro lado, é de salientar que a maioria destes processos judiciais se consubstanciam na violação de garantias muito específicas, que são regularmente repetidas nas pronúncias dos órgãos judiciais responsáveis pelo seu julgamento. Trata-se, fundamentalmente, da transgressão dos princípios do non-refoulement e do direito à tutela jurisdicional efectiva, doutrinas cuja salvaguarda, no quadro europeu, está consagrada nos artigos 3.º e 13.º da CEDH; bem como da proibição de expulsões colectivas de estrangeiros, protegida no artigo 4.º do Protocolo n.º 4 da Convenção. No entanto, estes processos judiciais são morosos e muito complexos, e as suas decisões estão muitas vezes em conflito direto com decisões anteriores de outros tribunais ou mesmo dos próprios órgãos que as proferem. Por estas razões, é também essencial que os órgãos responsáveis pela representação e defesa dos Estados soberanos conheçam profundamente o direito internacional e

¹⁸ Praticamente todos estes pronunciamentos provêm de esferas nacionais, dado que o TEDH evita pronunciamentos categóricos sobre a segurança dos Estados e dá prioridade a uma análise caso a caso, tal como os tribunais superiores espanhóis. Por outro lado, vários países europeus elaboraram listas de países terceiros seguros, incluindo Marrocos em algumas delas, como é o caso, por exemplo, dos Países Baixos (Immigration and Naturalisation Service, 2018). Esta prática está a ganhar terreno entre os Estados europeus e está em consonância com as disposições do Pacto de Migração e Asilo, que introduziu este conceito no novo Regulamento de Procedimentos de Asilo (Regulamento (UE) 2024/1348), que começará a ser aplicado a partir de 12 de junho de 2026 (Secção V, arts. 57.º e seguintes).

saibam compatibilizar tais doutrinas com o seu direito interno - propondo mesmo as necessárias alterações legislativas - de modo a assegurar, enquanto garantes da ordem jurídica, a conformidade das decisões que afectam a sua esfera de representação com o direito e a prática internacionais.

Por último, e em consonância com o exposto, não se pode ignorar a mutabilidade que caracteriza a interpretação da ordem jurídica internacional. Não se trata de uma fraqueza do sistema em si mesmo: as regras, sobretudo em ambientes anárquicos como o atual, estão em permanente processo de transformação, pelo que os operadores jurídicos não têm outra alternativa senão adaptar as suas posições às realidades existentes, o que tem sido feito desde a Antiguidade, quando existiam figuras jurídicas impensáveis no mundo contemporâneo. Neste sentido, um cenário tão volátil como o que rege a atual geopolítica mundial exige - no respeito pelos consensos inerentes à manutenção da paz e segurança internacionais, entre os quais se encontra a consideração da dignidade da pessoa humana como fonte inalienável dos direitos humanos - uma certa margem na interpretação das normas que regem as obrigações dos Estados, posição que não é nova na doutrina (Koskeniemi, 2004). Desta forma, garante-se o cumprimento adequado das mesmas, respeitando a vontade dos seus promotores e favorecendo a coexistência, aprofundando assim o desenvolvimento de um ambiente internacional próspero para todos os seus habitantes.

REFERÊNCIAS BIBLIOGRÁFICAS

- Alarcón Velasco, N. (2015), El abogado ante las normas de asilo: vigilancia de su aplicación, Consejo General de la Abogacía Española. Disponível online: <https://www.abogacia.es/actualidad/noticias/el-abogado-ante-las-normas-de-asilo-vigilancia-de-su-aplicacion/>. [Acedido em: 31/03/2025].
- Carrasco Durán, M. (2020). La definición constitucional del derecho a la tutela judicial efectiva, in *Revista de derecho político*, núm. 107, 13-40.
- Cole, P. (2012), *Borderline Chaos? Stabilizing Libya's Periphery*, Médio Oriente, outubro de 2012, Washington: Carnegie Endowment for International Peace.
- Comissão Espanhola de Ajuda aos Refugiados (3 de outubro de 2017), Tribunal Europeu dos Direitos do Homem condena Espanha por dois "regressos a quente". Disponível em linha: <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>. [Acedido em 31/03/2025].
- Comissão Europeia (2022), Relatório sobre o estado de Schengen 2022, Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, COM(2022) 301 final. Disponível em linha: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022DC0301>. [Acedido em: 31/03/2025].
- Comissão Europeia (2024), Eurobarómetro Standard. Europeans' opinions about the European Union's priorities, n.º 102, Bruxelas: Serviço das Publicações da UE. Disponível em linha: <https://europa.eu/eurobarometer/surveys/detail/3215>. [Acedido em 31/03/2025].
- Conselho da União Europeia (2015), Conclusões do Conselho sobre o Processo de Paz no Médio Oriente. Disponível em linha: <https://www.consilium.europa.eu/en/press/press-releases/2015/07/20/fac-mepp-conclusions/pdf/>. [Acedido em 31/03/2025].
- Consejo General de la Abogacía Española (3 de outubro de 2017), La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH. Disponível em linha: <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>. [Acedido em 31/03/2025].
- Curzon, G. (1907), *Frontiers*, Oxford: Clarendon Press.
- Del Valle Gálvez, A. (2019), La fragilidad de los derechos humanos en las fronteras exteriores europeas, y la externalización/ extraterritorialidad de los controles migratorios in *Anuario de los cursos de derechos humanos de Donostia-San Sebastián*, Vol. XVIII, Valencia: Tirant lo Blanch.
- Doebbler, C. (2018), *Dictionary of Public International Law*, Londres: Row-man & Littlefield.

- Eurostat (2025), População em 1 de janeiro por grupo etário, sexo e nacionalidade. Disponível em linha: https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en. [Acedido em 31/03/2025].
- Freedman, J. (2024), *The violent externalisation of asylum* in *Research Handbook on Asylum and Refugee Policy*, pp. 204-220, Cheltenham: Edward Elgar Publishing.
- Frontex (2021), *Risk Analysis for 2021*, Varsóvia. Disponível em linha: <https://www.frontex.europa.eu/publications/risk-analysis-for-2021-MmzGl0>. [Acedido em 31/03/2025].
- Frontex (2024), *Annual Brief 2023*, Varsóvia. Disponível em linha: <https://prd.frontex.europa.eu/document/annual-brief-2023/>. [Acedido em 31/03/2025].
- Golmayo, P. B. (1866), *Instituciones de Derecho Canónico*, Madrid: Imprenta de A. Peñuelas.
- Harris Díez, R. (2011), *El paisaje de los dioses: los santuarios griegos de la época clásica y su entorno natural*, in *AISTHESIS: Revista Chilena de Investigaciones Estéticas*, núm. 49, Santiago de Chile: Instituto de Estética de la Pontificia Universidad Católica de Chile.
- Hathaway, J. C. (2005), *The rights of refugees under International Law*, Cambridge: Cambridge University Press.
- Infante Caffi, M.T. (2016), *Las fronteras desde la perspectiva del Derecho Internacional*, in *Revista de Estudios Internacionales*, núm. 185, pp. 59-86, Santiago: Instituto de Estudios Internacionales de la Universidad de Chile. Disponível online: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692016000300004. [Acedido em: 31/03/2025].
- Kamto, M. (2007), *Third report on the expulsion of aliens*, Genebra: Comissão de Direito Internacional das Nações Unidas.
- Koskenniemi, M. (2004), *The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870-1960*, Cambridge: Cambridge University Press.
- Lacan, J. (1966), *Écrits*, Paris: Éditions du Seuil.
- Martínez Escamilla, M. (2021), *Las "devoluciones en caliente" en el asunto N. D. y N.T. contra España* (Sentencia de la Gran Sala TEDH de 13 de febrero de 2020) in *Revista Española de Derecho Europeo*, Núm. 77.
- Gabinete do Alto Comissariado para os Direitos Humanos (2018), *Recommended Principles and Guidelines on Human Rights at International Borders*, Genebra: ACNUR. Disponível em linha: <https://acnurdh.org/principios-y-directrices-recomendados-sobre-los-derechos-humanos-en-las-fronteras-internacionales/>. [Acedido em 31/03/2025].

Parlamento Europeu (2015), Resolução do Parlamento Europeu sobre o papel da UE no processo de paz no Médio Oriente. Disponível em linha: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0318_EN.html. [Acedido em: 31/03/2025].

Real Academia Española (2014), Diccionario de la lengua española (23ª edição).

Real Academia Española, Diccionario panhispánico del español jurídico (DPEJ). Disponível em linha: <https://dpej.rae.es/>. [Acedido em 31/03/2025].

RTVE (3 de outubro de 2017), O Tribunal Europeu dos Direitos Humanos condena a Espanha por duas "devoluções quentes" em Melilla. Disponível online: <https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml>. [Acedido em: 31/03/2025].

Sánchez Tomás, J. M. (2018), Las "devoluciones en caliente" en el Tribunal Europeo de Derechos Humanos (STEDH, As. N.D. Y N.T. vs España, de 03.10.2017), in *Revista Española de Derecho Europeo*, núm 65, pp. 102-135.

Sanz Donaire, J. J. (2023). Del concepto de frontera, in *Boletín de la Real Sociedad Geográfica*, Número extraordinario 2023, pp. 253-262. <https://doi.org/10.22201/cei-ich.24485691e.2014.12.49710>.

Serviço de Imigração e Naturalização (2018), Beoordeling veilige derde landen - Marokko, Informatiebericht SUA IB 2018/105. Disponible en línea: https://puc.overheid.nl/ind/doc/PUC_9890080000_1/1?solrID=PUC_9890080000_1_1&solrQ=morocco. [Acedido em 31/03/2025].

Soler García, C. (2017), A Guarda Europeia de Fronteiras e Costeira: Um avanço sobre a Frontex? Una valoración provisional, in *Revista Eletrónica de Estudios Internacionales*, núm. 34. Disponível online: <https://www.reei.org/index.php/revista/num34/articulos/guardia-europea-fronteras-costas-avance-respecto-frontex-una-valoracion-provisional>. [Acedido em: 31/03/2025].

Zaidman, L. B., Schmitt-Pantel, P. (2002), *La religión griega en la polis de la época clásica* (Díez Platas Trad.), Colmenar Viejo: Akal.

LEGISLAÇÃO E JURISPRUDÊNCIA

Carta das Nações Unidas (1945), Conferência das Nações Unidas sobre Organização Internacional, assinada em São Francisco em 26 de junho de 1945.

Convenção sobre os Direitos e Deveres dos Estados (1933), Sétima Conferência Internacional Americana de Montevideú, Série de Tratados da Liga das Nações, volume 165, página 19.

Convenção relativa ao Estatuto dos Refugiados (1951), Conferência das Nações Unidas de Plenipotenciários sobre o Estatuto dos Refugiados e Apátridas, assinada em Genebra em 28 de julho de 1951, Série de Tratados das Nações Unidas, Volume 189, página 137.

Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (1950), feita em Roma em 4 de novembro de 1950.

Protocolo relativo ao Estatuto dos Refugiados (1967), assinado em Nova Iorque em 31 de janeiro de 1967, Série de Tratados das Nações Unidas n.º 8791, Vol. 606, p. 267.

Decreto legislativo del 19 novembre 2007, n. 251, Attuazione della direttiva 2004/83/CE recante norme minime sull'attribuzione, a cittadini di Paesi terzi o apolidi, della qualifica del rifugiato o di persona altrimenti bisognosa di protezione internazionale, nonché norme minime sul contenuto della protezione riconosciuta.

Diretiva 2011/95/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, que estabelece normas relativas às condições a preencher por nacionais de países terceiros ou apátridas para poderem beneficiar de proteção internacional.

Diretiva 2013/32/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional.

Diretiva 2013/33/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que estabelece normas em matéria de acolhimento dos requerentes de proteção internacional.

Lei 12/2009, de 30 de outubro, que regula o direito de asilo e a proteção subsidiária.

Regulamento (UE) n.º 604/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida.

Regulamento (UE) 2024/1348 do Parlamento Europeu e do Conselho, de 14 de maio de 2024, que estabelece um procedimento comum de proteção internacional na União e que revoga a Diretiva 2013/32/UE.

Tribunal Europeu dos Direitos do Homem (1997), caso H.L.R. contra França, Acórdão (Grande Secção) de 29 de abril de 1997.

Tribunal Europeu dos Direitos do Homem (2012), Hirsi Jamaa e outros v. Itália Acórdão (Grande Secção) de 23 de fevereiro de 2012.

Tribunal Europeu dos Direitos do Homem (2015), caso N. D. e N. T. contra Espanha, Decisão (Terceira Secção) de 7 de julho de 2015.

Tribunal Europeu dos Direitos do Homem (2017), caso N. D. e N. T. v. Espanha, Acórdão (Terceira Secção) de 3 de outubro de 2017.

Tribunal Europeu dos Direitos do Homem (2020), Processo N.D. e N.T. contra Espanha, Acórdão (Grande Secção) de 13 de fevereiro de 2020.

Tribunal Permanente de Justiça Internacional (1933), Legal status of Eastern Greenland, Judgment of 5 April, Series A./B., Fascicle No. 53, Leiden: A. W. Sijthoff's Publishing Company.

Tribunal Internacional de Justiça (2002), Affaire relative à la souveraineté sur Pulau Ligitan et Pulau Sipadan, Acórdão de 17 de dezembro, Vendas nº 858.

Tribunal Internacional de Justiça (2012), Questões relativas à obrigação de perseguir ou extraditar (Bélgica v. Senegal), Acórdão de 20 de julho de 2012,

Tribunal Permanente de Arbitragem de Haia (1998), Territorial Sovereignty and Scope of the Dispute (Eritrea and Yemen), sentença de 9 de outubro, in Reports of International Arbitral Awards, Volume XXII pp. 209-332.

Tribunal Penal Internacional para a ex-Jugoslávia (2001), Procurador v. Dragoljub Kunarac Radomir Kovac e Zoran Vukovic, Acórdão de 22 de fevereiro de 2001.

Audiência Nacional (2018), Acórdão 1441/2018, 15 de março de 2018.



Artigo de investigação

A GUERRA DE NIXON CONTRA A DROGA E A ASCENSÃO DA VIGILÂNCIA VIRTUAL DAS FRONTEIRAS NOS ESTADOS UNIDOS

Tradução para o português com ajuda de IA (DeepL)

J. Luigi M. Kunz Saponaro

Investigador doutorado na Universidade Carlos III de Madrid.

Mestrado em Geopolítica e Estudos Estratégicos.

Mestrado em Segurança, Defesa e Geoestratégia.

jkunz@hum.uc3m.es

Recebido em 31/03/2025

Aceite em 21/05/2025

Publicado em 27/06/2025

Citação recomendada: Kunz Saponaro, J. L. M. (2025). A guerra às drogas de Nixon e o surgimento da vigilância virtual de fronteiras nos Estados Unidos. *Revista Logos da Guarda Civil*, 3(2), p.p. 147-170.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

A GUERRA DE NIXON CONTRA A DROGA E O AUMENTO DA VIGILÂNCIA VIRTUAL DAS FRONTEIRAS NOS EUA

Resumo: INTRODUÇÃO. 2. REVISÃO BIBLIOGRÁFICA SOBRE FRONTEIRAS E VIGILÂNCIA VIRTUAL. 3. 3. A TEORIA DA SEGURANÇA COMO QUADRO TEÓRICO. 3.1 Título da subsecção três, ponto um. 3.2. 4. OPERACIONALIZAÇÃO E METODOLOGIA 5. ANÁLISE 5.1 . A criação de uma Questão de Segurança por Nixon. 5.1.1 A criação de uma Guerra Nacional contra a Droga. 5.1.2 A virtualização da fronteira durante o mandato de Nixon. 5.2. Resultados e efeitos aplicados da securitização de Nixon. 6. CONCLUSÃO. 7. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: Este artigo investiga a evolução da fronteira entre os EUA e o México, de uma fronteira historicamente simbólica para uma das fronteiras mais fortificadas e tecnologicamente avançadas do mundo. Nas últimas décadas, assistiu-se a uma transformação significativa das práticas de controlo fronteiriço, caracterizada pela integração de mecanismos de vigilância digital que reforçam as barreiras físicas tradicionais. Este estudo aborda este fenómeno, explorando o nexu entre a Guerra contra a Droga de Nixon e a digitalização da fronteira EUA-México durante a Administração Nixon (1969-1974). Concebendo a crise da droga como uma ameaça existencial, a retórica do Presidente Nixon definiu as drogas como "inimigo número um", dando assim início à sua Guerra contra a Droga. Assim começou um processo de securitização que permitiu a afetação de recursos extraordinários para combater esta nova ameaça. Utilizando a teoria da securitização desenvolvida pela Escola de Copenhaga, é analisado o papel desempenhado por Nixon no enquadramento da ameaça à segurança, a fim de elucidar a forma como o seu discurso justificou a criação de práticas virtuais de controlo das fronteiras nos Estados Unidos. Os resultados sugerem que a securitização da crise da droga forneceu a base necessária para a adoção de tecnologias inovadoras de vigilância digital. Esta investigação contribui para o debate académico sobre a digitalização das fronteiras e fornece um quadro metodológico para estudos comparativos sobre a evolução virtual das fronteiras nacionais.

Resumen: Este trabajo investiga la evolución de la frontera entre Estados Unidos y México, que pasó de ser históricamente un límite simbólico para convertirse en una de las fronteras más fortificadas y tecnológicamente avanzadas del mundo. En las últimas décadas se ha observado una transformación significativa en las prácticas de control fronterizo, caracterizada por la integración de mecanismos de vigilancia digital que refuerzan las barreras físicas tradicionales. El estudio que se presenta aborda este fenómeno explorando el nexu entre la Guerra contra las Drogas de Nixon y la digitalización de la frontera entre Estados Unidos y México durante la Administración Nixon (1969–1974). Al conceptualizar la crisis de las drogas como una amenaza existencial, la retórica del presidente Nixon definió las definió como el “enemigo número uno”, iniciando así su Guerra contra las Drogas. Comenzó así un proceso de securitización que permitió asignar recursos extraordinarios para contrarrestar esta nueva amenaza percibida. Mediante el uso de la teoría de la securitización desarrollada por la Escuela de Copenhague, se analiza el papel desempeñado por Nixon al enmarcar la amenaza de seguridad, con el fin de dilucidar cómo su discurso justificó la creación de prácticas de control fronterizo virtual en Estados Unidos. Los hallazgos sugieren que la securitización de la crisis de las drogas proporcionó la base necesaria para adoptar tecnologías

innovadoras de vigilancia digital. Esta investigación contribuye al debate académico sobre la digitalización de fronteras y ofrece un marco metodológico para estudios comparativos sobre la evolución virtual de las fronteras nacionales.

Palavras-chave: Fronteira EUA-México, Vigilância Digital, Teoria da Securitização, Guerra contra a Droga, Administração Nixon.

Palabras clave: Frontera EE. UU.-México, Vigilancia Digital, Teoría de la Securitización, Guerra contra las Drogas, Administración Nixon.

1. INTRODUÇÃO

A fronteira que separa os Estados Unidos da América (EUA) do México é uma das mais longas do mundo. Uma série de montanhas, desertos e rios caracterizam os 3.141 quilómetros de terreno que separam os dois países. As primeiras demarcações físicas da fronteira foram introduzidas com o fim da Guerra EUA-México de 1847, que resultou no Tratado de Guadalupe (ver Trist *et al.*, 2022). As alterações políticas introduzidas por este Tratado foram transferidas para o território através de 52 montes de pedra colocados de costa a costa ao longo de toda a margem (US Customs and Border Protection, 2019). Muito mudou desde a separação simbólica que demarca a fronteira sul dos Estados Unidos (EUA). Atualmente, tornou-se uma das fronteiras mais fortificadas e tecnologicamente avançadas que existem.

O aspeto virtual desta fronteira é de particular interesse para as práticas de vigilância que os países de todo o mundo efectuam para proteger as suas fronteiras. Com efeito, o potencial dos sistemas de vigilância contemporâneos em termos de controlo das fronteiras nacionais foi objeto de numerosos estudos até há pouco tempo (ver Adams, 2001; Amoores, Marmura, & Salter, 2008; Heyman, 2008). No entanto, pouco se sabe sobre quando e porquê, em particular, os Estados Unidos decidiram entrelaçar os aspectos físicos e virtuais das suas fronteiras, a fim de melhorar o seu controlo. Trata-se de um parêntesis intrigante, especialmente tendo em conta a posição de liderança dos Estados Unidos em termos do arsenal digitalizado utilizado ao longo da fronteira EUA-México, juntamente com uma consideração bastante escassa sobre onde tudo começou.

A investigação mostra uma ligação entre a Guerra do Vietname e a implementação pelos EUA de mecanismos virtuais de aplicação da lei ao longo da fronteira entre os EUA e o México (ver Barkan, 1972; Grandin, 2019; Rosenau, 2001). No entanto, não foi dada atenção suficiente ao nexos que liga estes dois acontecimentos distintos da história americana. Para ser mais preciso, o nexos em questão é a Guerra às Drogas de Nixon. Foi ao descrever a droga como o inimigo número um dos Estados e ao declarar uma guerra total contra a droga em 1971 que o Presidente conseguiu abrir uma janela para a digitalização da fronteira sul. Ao abordar a seguinte questão de investigação, este artigo pretende preencher esta lacuna na literatura académica: de que forma a Guerra contra a Droga durante a Administração Nixon contribuiu para a transição do controlo fronteiriço físico ao longo da fronteira sul para mecanismos de aplicação virtual?

Uma ferramenta valiosa para encontrar uma resposta a esta questão é oferecida pela teoria da securitização. Esta teoria foi criada pela Escola de Copenhaga e fornece um quadro teórico que pode ser utilizado para identificar padrões no processo de securitização de uma questão que fornece recursos extraordinários de compensação. Nesta investigação, estes padrões elucidados por um dos principais componentes da Escola, Wæver (1995), são aplicados aos comentários de Nixon sobre a Guerra contra a Droga e ao subsequente investimento em activos digitais para a fronteira sul dos EUA.

Este estudo defende que o facto de Nixon ter enquadrado o discurso sobre a droga como uma ameaça nacional permitiu aos Estados Unidos avançar com a virtualização da fronteira entre os EUA e o México. O período de tempo em análise neste trabalho coincide com o mandato da Administração Nixon, ou seja, 1969-1974. Estabelecer em que momento exato e de que forma os Estados Unidos conseguiram iniciar a sua fortificação virtual da fronteira é valioso para o debate académico. Isto porque os resultados desta

investigação podem ser utilizados para comparar os desenvolvimentos tecnológicos nos estudos fronteiriços de outros países também durante as suas fases iniciais de virtualização das fronteiras.

A fim de desenvolver a investigação de forma diligente, o presente documento está dividido nas secções seguintes. A primeira secção inclui a revisão da literatura sobre as abordagens teóricas mais relevantes que foram adoptadas para realizar estudos sobre fronteiras virtuais. A segunda secção apresenta a teoria da securitização como o quadro teórico adotado por este estudo para levar a cabo a sua análise. A terceira secção resume a operacionalização e a metodologia utilizadas para formalizar esta investigação. A quarta secção consiste na análise deste estudo. Nesta secção, os princípios da teoria da securitização são aplicados a dois dos discursos emblemáticos de Nixon. As conclusões resultantes são depois discutidas com base no apoio de fontes secundárias. A última secção propõe uma conclusão que sintetiza os resultados e as considerações alcançadas ao longo deste estudo.

2. REVISÃO DA LITERATURA SOBRE FRONTEIRAS E VIGILÂNCIA VIRTUAL

Existem várias teorias que são utilizadas para apreciar os vários fundamentos das fronteiras e os seus padrões de transformação. No que respeita especificamente aos processos de virtualização das fronteiras, o âmbito das teorias que se aplicam é consideravelmente mais restrito. Para identificar o que tem sido escrito sobre a relação das fronteiras e a sua digitalização de acordo com as necessidades políticas, quatro teorias principais conseguem captar a atenção. Esta secção é dedicada à discussão destas diferentes contribuições académicas. Cada uma delas traz uma visão diferente sobre o tema de investigação do estudo e pode ser utilizada para compreender a sua origem.

Michel Foucault impulsionou uma perspetiva mais filosófica nos estudos de vigilância. Ao rever a teoria do filósofo francês, Lemke (2015) afirmou que "o trabalho de Foucault sobre a governamentalidade não só oferece percepções importantes para uma análise do Estado, mas também fornece ferramentas analíticas para investigar a relação entre as tecnologias liberais e de segurança" (p. 5). Mais especificamente, a teoria da governamentalidade foucaultiana descreve como os Estados empregam o poder através de técnicas disciplinares e de vigilância, em vez da força direta (Lemke, 2015). Esta teoria analisa a dimensão extraterritorial do controlo fronteiriço gerido por agentes estatais que podem ir além da demarcação física do seu próprio país.

Esta ideia é atractiva para compreender a digitalização das fronteiras, uma vez que pode ser aplicada às práticas estatais que combatem as ameaças à segurança nacional através da reinterpretação das demarcações físicas. A ideia subjacente a esta teoria é tentar bloquear riscos específicos antes de estes chegarem à fronteira. Mais concretamente, as leis nacionais podem ser utilizadas para promover alterações governamentais que prevejam a informatização das questões de segurança que ameaçam a segurança nacional. Desta forma, os Estados podem avançar para um sistema de vigilância cada vez mais virtual, utilizado para monitorizar e eliminar os perigos antes de estes conseguirem entrar no seu território (ver Armstrong, 1992; Paden, 1984). Este conjunto de acções mostra como as fronteiras convencionais podem mudar quando as configurações virtuais são integradas nas práticas de controlo das fronteiras.

A teoria foucaultiana da governamentalidade, no entanto, fica aquém quando aplicada à investigação da securitização das fronteiras relacionadas com a droga. Embora a teoria mencione a agência tecnológica na criação de fronteiras, está principalmente orientada para um estudo da vigilância e do controlo, em vez de se centrar na securitização das fronteiras *em si*. Esta teoria não é capaz de explicar por que razão os decisores políticos actuam quando confrontados com acontecimentos imprevistos, como foi o caso da crise da droga dos anos 60 nos Estados Unidos. Neste sentido, Kerr (1999) concluiu que a teoria não consegue "explicar os limites mutáveis do governo, para além de apontar para o simples facto de o governo falhar frequentemente devido a resultados não planeados" (p. 196). Assim, embora esta governamentalidade foucaultiana se tenha revelado pioneira na virtualização das fronteiras, não permite responder de forma exhaustiva à questão de investigação que orienta o presente estudo.

Outra teoria relevante utilizada para analisar as fronteiras inteligentes é o determinismo tecnológico. Esta teoria baseia-se na identificação dos desenvolvimentos tecnológicos como factores sociais e políticos. Em particular, salienta a importância da tecnologia na modelação da mudança política. Nas palavras de Smith (1994), "o poder da tecnologia [é] um agente crucial de mudança [que] ocupa um lugar de destaque na cultura da modernidade" (p. ix). De acordo com esta teoria, o impulso que faz com que as novidades aconteçam não é impulsionado pelas pessoas, mas pela própria tecnologia. Esta, por sua vez, provoca mudanças que são primeiro colocadas na agenda política e depois implementadas pelos decisores políticos.

Deste modo, as transformações das fronteiras são entendidas como o resultado de avanços tecnológicos e não de impulsos sociopolíticos. Neste sentido, o surgimento da vigilância eletrónica, juntamente com o rastreio biométrico e a deteção remota, tornou a aplicação da lei virtual viável em primeiro lugar. Assim, ligando esta perspetiva à questão de investigação deste artigo, as estratégias de aplicação da lei em matéria de droga evoluíram em resultado de possibilidades tecnológicas e não de decisões políticas. Consequentemente, os decisores políticos dos EUA foram pressionados, em vez de impulsionarem a mudança tecnológica, a implementar a aplicação da lei nas fronteiras virtuais para combater a entrada de droga no país.

Embora o determinismo tecnológico consiga fornecer informações relevantes sobre a mudança dos regimes fronteiriços, tem sido criticado por simplificar demasiado este processo. É amplamente argumentado que os membros sociais e políticos também são capazes de influenciar a tecnologia em vez de estarem à sua mercê. Ou seja, uma compreensão mais profunda da tecnologia tornou possível o seu controlo (Dafoe, 2015, p. 1049; Lynch, 2008). Consequentemente, o aspeto digital das fronteiras não é o resultado do impulso tecnológico, mas é controlado pelos políticos. Assim, a adaptação da fronteira sul dos EUA durante o mandato de Nixon pode ser vista como uma viragem tecnológica clara. No entanto, esta viragem foi controlada por acções masculinas, o que torna difícil confiar no determinismo tecnológico para a investigação proposta neste documento.

A composição digital das fronteiras também pode ser compreendida através da teoria das fronteiras de Nail. Esta teoria oferece uma visão da fronteira que vê uma qualidade cada vez mais móvel e dispersa nas fronteiras físicas convencionais. Na opinião de Nail (2016), "a fronteira não é redutível à definição clássica dos limites de um Estado soberano" (p. 2). As fronteiras, observou o autor, estão inevitavelmente a evoluir para

uma identidade informacional ou digital que afecta a compreensão social de um país. Isto significa que as fronteiras assumiram uma forma virtual, uma vez que os problemas modernos afectam a circulação transfronteiriça de pessoas e bens, para os quais são necessárias respostas actualizadas. No caso do tráfico de droga nos Estados Unidos, por exemplo, os novos métodos adoptados pelos cartéis exigiram acções inovadoras do controlo das fronteiras americanas para contrariar esta tendência. Nos anos 60 e 70, estas acções reduziram-se à transformação das fronteiras em espaços de controlo em rede.

A teoria das fronteiras contorna, portanto, a concepção convencional das fronteiras enquanto tais. Em vez de se concentrar exclusivamente no seu aspeto territorial e físico, como elucidado por Sharma (2023, pp. 163-164), é necessário alargar esta concepção aos activos intangíveis que constituem as fronteiras dos Estados. As implicações desta teoria acrescentam uma nova dimensão ao poder dos governos. Ou seja, as fronteiras não devem ser vistas como uma simples linha, mas como uma ampla área que circunda a demarcação física (Nails, 2016). De facto, os Estados podem ir muito além das suas fronteiras físicas através de mecanismos de aplicação virtual com o objetivo de securitizar as suas fronteiras. Os modelos práticos são as bases de dados da Patrulha de Fronteiras dos EUA e as redes de partilha de informações que têm sido amplamente utilizadas para proteger a sua fronteira sul. Na década de 1970, estes sistemas de patrulha fronteiriça conduziram a expansões que abriram caminho às actuais estruturas digitais de aplicação das fronteiras.

A teoria das fronteiras defende a ideia de que os Estados podem monitorizar os movimentos para além das suas próprias fronteiras. As delimitações territoriais, de acordo com esta concepção, tornam-se menos relevantes para que os governos tomem medidas relacionadas com a vigilância das fronteiras (Sharma, 2023. P. 164). Embora continuem a representar um aspeto importante da política de fronteiras, os governos tendem a agir para além da delimitação territorial, a fim de intercalar potenciais ameaças. Por outras palavras, a prevenção torna-se tão importante como a dissuasão física. As armadilhas desta mentalidade são as intervenções políticas extraterritoriais susceptíveis de prejudicar as relações internacionais. Esta teoria é útil para compreender a mudança geral na concetualização da fronteira sul dos EUA. No entanto, pode ser utilizada para estudar a separação social, embora não tenha uma ligação clara com as questões de segurança das fronteiras.

Para compreender as fronteiras de um ponto de vista relacionado com a segurança, a teoria da securitização da escola de Copenhaga deve ser tida em conta. Otukoya (2024, p. 1750) observou que a criação de um problema de segurança pode ser a chave para a criação de recursos extraordinários utilizados para proteger uma nação de um perigo imaginado. Esta teoria é útil para compreender como os recursos digitais são utilizados para reforçar o aspeto físico da fronteira. Neste caso, a atenção centra-se, entre outras coisas, nos sensores de movimento, na videovigilância e em quaisquer outras características tecnológicas que são utilizadas para policiar a fronteira territorial com maior eficácia. Por conseguinte, é apresentado como o quadro teórico adequado necessário para identificar esses padrões ao longo da fronteira sul dos Estados Unidos.

Olhando para os primórdios da Guerra contra a Droga, manobras como a Operação Intercetar, lançada em 1969, foram justificadas como uma ação necessária para combater o inimigo público número um da América na altura. Nesta operação, novas formas de vigilância eletrónica das fronteiras tornaram-se necessárias pela primeira vez na história do regime fronteiriço dos Estados Unidos. Estas necessidades constituem os pilares

fundamentais da complexa dimensão tecnológica que caracteriza a fronteira americana contemporânea. Dada a estreita relação entre esta teoria da securitização e os objectivos da presente investigação, é necessário desenvolver a sua composição. Na secção seguinte, a teoria da securitização é resumida. Esta fornece indicadores-chave para compreender como a securitização da fronteira dos EUA mudou durante a administração Nixon, adoptando um aspeto virtual.

3. A TEORIA DA TITULARIZAÇÃO COMO QUADRO TEÓRICO

A teoria da securitização é um quadro útil que pode ser utilizado para compreender a segurança das fronteiras nos Estados Unidos durante a presidência de Nixon. A função geral desta teoria é explicar a forma como as questões passam a orientar o processo de tomada de decisões de um país em matérias como o controlo das fronteiras. Aplicada ao estudo em questão, esta teoria parece ser de grande ajuda para compreender os mecanismos de controlo virtual que os Estados Unidos acrescentaram à sua fronteira física meridional. Aplicando a teoria da securitização a este tópico, este estudo procura elucidar o papel que o Presidente Nixon desempenhou na contribuição para a implementação de uma fronteira virtual. Esta secção é dedicada a delinear os principais princípios da teoria da securitização, a fim de os aplicar formalmente à análise do documento.

A escola de Copenhaga baseou a sua teoria em cinco pilares principais. Os pilares em questão são (1) a securitização como ato de fala, (2) o enquadramento elitista das ameaças, (3) a exigência de aceitação por parte da audiência, (4) a identificação do objeto referente e (5) a reversibilidade e a dessecuritização. Todos estes factores combinados podem ser utilizados na análise do presente documento para descobrir como a Guerra contra a Droga dos EUA contribuiu para a transição do controlo físico das fronteiras para mecanismos virtuais de aplicação da lei. No entanto, antes de passar à análise, cada indicador é resumido e contextualizado para clarificar a sua utilização no estudo de caso da revisão.

Declarar um problema como uma ameaça à segurança é um ato performativo realizado por um governo. Com esta conceção de segurança, Ole Wæver - o mentor da teoria da securitização - descobre um ato performativo que os governos realizam quando assinalam ao público a presença de um problema relacionado com a segurança (Wæver, 1995, p. 52). Ao chamar a atenção para um problema, uma elite pode realizar um ato que abre uma janela para medidas políticas excepcionais destinadas a impedir um determinado revés. É irrelevante se esta questão representa um problema comum ou uma ameaça real à segurança nacional. O que importa é que o público conceda aos representantes do Estado uma liberdade de ação considerável que legitime as suas acções. É a isto que se chama um ato de fala.

Os actos de fala baseiam-se na criação vertical de confiança entre os funcionários do Estado e os cidadãos. O sucesso de um ato de fala depende da medida em que uma promessa ou declaração é aceite pelo público. Os representantes do Estado aproveitam o sentimento de confiança que os cidadãos lhes transmitem para criar uma nova realidade política cuja existência depende da questão da segurança concebida. É através da utilização de actos de fala que se revela a legitimação para tomar medidas para enfrentar as ameaças à segurança. Esta legitimação, por sua vez, permite mobilizar o desbloqueamento dos recursos do Estado através da criação de acções que ultrapassam os

procedimentos normais e permitem a formação de medidas extraordinárias (Wæver, 1995, p. 53).

No entanto, esta prática não é isenta de riscos. Wæver (1995) sublinha que isto acontece porque torna difícil distinguir entre o ato e o grau real de ameaça que um país enfrenta (p. 6). Por outras palavras, o Estado pode tornar-se vítima da sua própria narrativa ao atribuir demasiada importância a uma questão que, na realidade, não representa um perigo real para a segurança da nação. Ao fazê-lo, pode ter o efeito oposto de comprometer a segurança do país, concentrando-se demasiado num problema inexistente e negligenciando as suas verdadeiras prioridades.

O segundo indicador recuperado na teoria da securitização é a prática das elites de enquadrar as ameaças. A teoria da securitização sublinha a influência que os principais actores têm na definição das acções políticas. Este processo é iniciado por aqueles poucos escolhidos que têm uma influência significativa nas altas esferas políticas. Quando estes indivíduos conseguem criar uma narrativa de ameaça, assumem o poder de definir o que pode ser definido como perigos existenciais para a segurança do país. O resultado é uma ação estatal coesa destinada a resolver o problema resultante da criação dessa mesma narrativa.

No entanto, a autoridade exercida pela elite é uma faca de dois gumes. Por um lado, permite uma reação rápida do Estado (Wæver, 1995, p. 54). Este facto é particularmente positivo, uma vez que os Estados são frequentemente limitados por uma burocracia complexa que prolonga consideravelmente o tempo de implementação das medidas oficiais. Por outro lado, este domínio permite que as elites contornem os processos democráticos convencionais (Wæver, 1995, p. 54). Isto significa que, ao acelerar o processo normalmente lento de elaboração de políticas, apenas um grupo restrito de pessoas concentra nas suas mãos o poder de decisão. A implicação desta concentração de poder permite à elite não só decidir como lidar com as ameaças à segurança, mas também decidir o que deve ser considerado uma ameaça e o que não deve. Assim, o enquadramento das questões de segurança pode ser facilmente associado aos interesses estratégicos das elites (Wæver, 1995, p. 54). Por outras palavras, as elites podem decidir se agem para garantir a segurança pública ou os seus interesses pessoais.

Isto leva-nos ao terceiro indicador: a exigência de aceitação pública. Os movimentos de securitização, segundo a escola de Copenhaga, dependem da aceitação por parte das audiências relevantes. Os principais públicos de interesse para a elite são a opinião pública, os órgãos legislativos ou os parceiros internacionais. Todos eles - independentemente ou não - devem confiar na veracidade da narrativa da ameaça construída para criar o *impulso* necessário para a ação prática. Estas, por sua vez, segundo Wæver (1995, p. 53), permitem encontrar uma solução para a ameaça proposta. Sem a aceitação do público, mesmo as reivindicações de segurança mais convincentes podem falhar. Assim, a não aceitação de uma questão de segurança é contraproducente e gera um processo de dessacralização. O esforço da elite desapareceria assim à custa dos seus interesses estratégicos (Wæver, 1995, pp. 53-54). É por isso que o indicador da procura de aceitação por parte do público é proposto como um fator essencial. É necessário analisar em que medida a aprovação ou a contestação do público em relação a procedimentos invulgares pode autorizar ou impedir o afastamento das práticas democráticas tradicionais.

O quarto indicador que compõe a teoria da securitização pode ser identificado com a identificação do objeto de referência. O processo de securitização necessita de uma especificação clara do que está em causa. Neste caso, o que está em jogo é designado por objeto de referência. De acordo com Wæver (1995, p. 52), o objeto de referência é normalmente identificado com a integridade do Estado, a soberania ou a segurança dos seus cidadãos. O processo de definição do objeto de referência é crucial para a mobilização de recursos. De facto, uma delimitação clara do objeto traçado pelos actores securitários desbloqueia os meios materiais necessários para defender essa entidade particular contra uma alegada coerção existencial (Wæver, 1995, pp. 52-53). Esta delimitação clara é fundamental para que se possa recorrer a acções de exceção, pois determina o que deve ser defendido por todos os meios.

A reversibilidade e a dessecuritização constituem o último indicador da teoria da titularização. De acordo com a escola de Copenhaga, a securitização está sujeita a uma mudança constante. Quando o público se apercebe de que uma ameaça à segurança já não é existencial, pode reverter as medidas de securitização tomadas até então e transformar a questão de novo num debate político normal (Wæver, 1995, p. 55). Esta retração permite que a elite que enquadrou a questão seja posta em cheque. Esta reversibilidade mostra como as respostas de emergência temporárias podem ser desmanteladas depois de terem passado por uma acumulação momentânea. Por isso, Wæver (1995, pp. 54-55) sugeriu que o ato de securitização comporta riscos intrínsecos que são inerentes ao processo de securitização. Por outras palavras, as acções de titularização podem facilmente ir e vir, tornando difícil prever quais as futuras acções de segurança que um governo poderá tomar.

Em geral, os princípios que constituem a teoria da titularização proposta pela escola de Copenhaga são instrumentos de análise valiosos. É o caso, nomeadamente, do tema de investigação deste trabalho. A aplicação das ferramentas analíticas disponibilizadas por esta teoria pode facilitar a compreensão de como a Guerra contra a Droga pode ter sido transformada numa questão de segurança utilizada para criar espaço para medidas excepcionais. Com efeito, os princípios enumerados nesta secção ajudam a avaliar a transformação de práticas criminosas convencionais - como o contrabando e o consumo de droga - e de problemas de saúde em medidas excepcionais adoptadas pelos Estados para resolver estas questões. Os discursos das elites provocaram mudanças políticas significativas que resultaram em políticas sem precedentes que levaram à adoção de mecanismos virtuais de aplicação da lei para combater o tráfico de droga ao longo da fronteira sul dos Estados Unidos. A secção seguinte apresenta a operacionalização e a metodologia que este documento adopta para levar a cabo a sua análise.

4. OPERACIONALIZAÇÃO E METODOLOGIA

Toshkov (2016, p. 100) descreveu a operacionalização como a tradução de conceitos abstractos em noções concretas que podem ser observadas, classificadas e medidas empiricamente. Os princípios que compõem a teoria da securitização podem ser utilizados com o mesmo objetivo. Este documento operacionalizou quatro dos cinco conceitos-chave para compreender o papel da Guerra contra a Droga na contribuição para a transição dos EUA para as fronteiras virtuais. Os quatro indicadores que compõem a teoria e que são utilizados neste documento para analisar o estudo de caso são: (1) a securitização como ato de fala, (2) o enquadramento elitista das ameaças, (3) o requisito de aceitação da audiência e (4) a identificação do objeto de referência. O último princípio delineado na teoria da securitização - reversibilidade e dessecuritização - não é útil para esta investigação. Ou seja, este último princípio é útil para estudar a desconstrução de uma medida de segurança, uma parte que este estudo não pretende cobrir. No entanto, este facto não compromete a robustez deste trabalho, uma vez que os padrões que conduzem à securitização se mantêm inalterados.

Os quatro indicadores permitem-nos aprofundar a dimensão virtual que a fronteira sul dos EUA adquiriu durante o mandato de Nixon. Consequentemente, é encorajada uma reflexão qualitativa crítica sobre o tema da investigação, a fim de compreender a importância atual para os EUA de reforçar a digitalização ao longo da sua fronteira territorial com o México. Os cinco indicadores são, por conseguinte, de importância fundamental para identificar a razão pela qual a crise da droga conseguiu ser um fator-chave nos mecanismos de aplicação da fronteira virtual.

A metodologia deste trabalho também precisa de ser clarificada. Esta investigação consiste num estudo de caso único. Mais especificamente, analisa a fronteira sul dos Estados Unidos durante a presidência de Nixon. Os estudos de caso único permitem fornecer informações precisas sobre um caso específico, a fim de criar conhecimentos que podem depois ser aplicados a casos semelhantes. Por outras palavras, com esta investigação, o modelo de investigação pode depois ser utilizado em casos semelhantes para identificar padrões análogos de evolução no controlo virtual das fronteiras. A decisão de optar por este estudo de caso baseia-se no facto de os EUA se encontrarem entre os primeiros países que decidiram optar pela digitalização parcial das suas fronteiras. Por conseguinte, a justificação para a seleção do estudo de caso reside no interesse de acrescentar novas informações à lacuna de investigação académica existente sobre este tema.

Ao longo da análise do tema, é utilizada uma variedade de fontes primárias e secundárias. O objetivo de dispor de um vasto leque de informações provenientes de várias fontes ajuda a consolidar e a garantir a qualidade das conclusões desta investigação. Tal como acontece com as fontes primárias, são tidas em conta declarações políticas, artigos de jornais e discursos públicos. Nestas fontes podem ser reconhecidas características importantes da teoria da titularização. Já as fontes secundárias utilizadas neste estudo provêm de estudos académicos realizados sobre o tema da segurança das fronteiras, da segurança virtual e da guerra contra a droga. Trata-se de uma prática útil que permite situar as conclusões do estudo num debate académico mais vasto.

A análise do discurso constitui a espinha dorsal deste estudo. Examina informações extraídas de dois discursos proferidos por Nixon em relação à guerra contra as drogas.

Baseada num método qualitativo, a interpretação das fontes fornecidas ajuda a identificar os indicadores apresentados no quadro teórico. Os discursos políticos proferidos pelo Presidente dos Estados Unidos são, pois, fundamentais para a realização deste estudo. Além disso, a aplicação deste método de investigação permite testar a teoria utilizada neste estudo. Com efeito, ao aplicar os indicadores propostos pela teoria da titularização aos discursos, é possível compreender se existem, de facto, padrões nos discursos políticos que possam conduzir à titularização dos riscos construídos.

O horizonte temporal desta investigação baseia-se no mandato da Administração Nixon. Mais especificamente, o período considerado vai de 1969 a 1974. Este período de tempo restrito ajuda a dar espaço a uma série de acções-chave tomadas pelo Presidente dos EUA da época em relação aos mecanismos de controlo virtual ao longo da fronteira EUA-México.

5. ANÁLISE

5.1. A CRIAÇÃO DE UM PROBLEMA DE SEGURANÇA POR NIXON

A vigilância da fronteira entre os EUA e o México entre 1969 e 1974 centrou-se predominantemente no comércio ilegal de droga. A região de Sinaloa, no noroeste do México, começou a cultivar ópio a partir de imigrantes chineses na década de 1910. Desde então, o cartel de Sinaloa enriqueceu exportando a substância principalmente para os Estados Unidos. No entanto, com a geração hippie e o tráfico de marijuana, a importação ilegal de substâncias para os EUA tornou-se um problema para a sociedade (Grillo, 2013, p. 255). O problema da droga tornou-se a questão central em torno da qual o Presidente Nixon baseou a maior parte da sua atividade política. Para além disso, Timmons (2017, p. 15) chamou a atenção para o facto de Richard Nixon se ter tornado o primeiro presidente a prometer fechar a fronteira EUA-México às drogas ilegais. De facto, à medida que a guerra no Vietname prosseguia, "a Administração Nixon está silenciosamente a americanizar a tecnologia da guerra, e a guerra na frente interna intensifica-se" (Barkan 1972, p. 1).

A fim de aprofundar o papel de Nixon no início desta tendência, a primeira parte da análise é dedicada a uma análise do discurso de dois dos discursos do Presidente em questão. As comunicações em questão são *Remarks About an Intensified Program for Drug Abuse Prevention and Control* e *Special Message to the Congress on Drug Abuse Prevention and Control*. Ambos os discursos tiveram lugar em 17 de junho de 1971. Ambos os discursos tiveram lugar no mesmo dia e seguiram-se um ao outro. De facto, o primeiro resume a conferência de imprensa realizada para explicar o que mencionou durante o seu discurso ao Congresso.

Ambos os discursos são fundamentais para compreender como o enquadramento elitista de uma ameaça foi proposto a audiências políticas e públicas. Analisando-os de perto, é possível compreender como Nixon conseguiu desbloquear recursos extraordinários para combater a nova e construída ameaça existencial das drogas nos EUA. Ambos os discursos são apresentados em conjunto num documento fornecido pelo Departamento de Defesa dos EUA (2017). Após identificarmos os pontos mais relevantes de ambos, passamos a esclarecer a relevância que essas medidas singulares tiveram no processo de virtualização da fronteira sul dos EUA entre 1969 e 1974.

5.1.1 Criar uma guerra nacional contra a droga

Ao considerar os discursos de Nixon do ponto de vista da teoria da securitização, é necessário procurar um ato performativo. Este ato deve chamar a atenção do público para a existência de um problema relacionado com a segurança que põe em perigo o seu bem-estar. O Presidente Nixon fê-lo ao declarar corajosamente uma guerra total contra a droga. Na sua conferência de imprensa, depois de se dirigir ao Congresso com uma mensagem especial, abriu a sua comunicação afirmando que "o inimigo público número um dos Estados Unidos é o abuso de drogas" (Departamento de Defesa dos EUA, 2017, p. 1). Uma abertura tão bombástica foi cativante para o público. Ajudou a criar um sentimento de medo entre a população dos EUA, 15 anos após a catastrófica Guerra do Vietname. Não é de surpreender que, naqueles anos, qualquer referência a ameaças à segurança nacional, guerras e inimigos suscitasse facilmente sentimentos de paranoia e o desejo de agir.

Para propor a nova ameaça, Nixon teve de indicar em que é que ela consistia efetivamente. Fê-lo afirmando que:

Existem várias grandes categorias de drogas: as da família da canábida, como a marijuana e o haxixe; as utilizadas como sedativos, como os barbitúricos e certos tranquilizantes; as que elevam o humor e suprimem o apetite, como as anfetaminas; e as drogas como o LSD e a mescalina, frequentemente designadas por alucinogénios. Por último, existem os analgésicos narcóticos, como o ópio e os seus derivados, a morfina e a codeína. A heroína é fabricada a partir da morfina". (Departamento de Defesa dos EUA, 2017, p. 10).

É isto que a teoria da securitização identifica com a identificação do objeto de referência. Ao apontar e insistir em quem ou o que representa uma ameaça, o público pode identificar o problema e pressionar para que sejam tomadas medidas contra ele.

Além disso, o facto de se apresentar como um Presidente prudente ajudou a tornar o ato performativo mais convincente. Assim, declarou que "hesito sempre em trazer qualquer nova responsabilidade para a Casa Branca, [...] mas penso que este é um problema tão urgente [...] que tinha de ser trazido" (US Department of Defense, 2017, p. 2). Ao fazê-lo, Nixon procurou apresentar-se como o protetor e garante dos EUA, cujas acções eram guiadas pelas necessidades dos cidadãos norte-americanos e não por interesses pessoais.

Foi criada uma série de medidas de exceção para fazer face a esta ameaça à segurança nacional. Nixon afirmou que "uma nova ofensiva total deve ser empreendida" (Departamento de Defesa dos EUA, 2017, p. 1), evocando a necessidade de um esforço comum para deter um perigo que tinha conseguido penetrar em solo americano. Estas palavras clarificaram a medida em que os EUA estavam empenhados em combater ativamente as ameaças à segurança relacionadas com a droga. A implementação de medidas bélicas, como o destacamento e a criação de departamentos militares e federais para controlar e combater as rotas de entrada de droga nos Estados Unidos, constituiu a base deste novo plano de ação.

Neste ponto, é necessário sublinhar a aceitação pelo público do ato de fala de Nixon. De facto, pode dizer-se que o público aceitou o discurso adotado de War on Drugs. Sinais

dessa aceitação são uma série de acções propostas pela Administração e depois implementadas com o apoio geral da maioria do país. A operação mais emblemática que deu início à Guerra contra a Droga foi a Operação Interdição, lançada ao longo de setembro e outubro de 1969. Esta operação resultou no encerramento quase total da fronteira entre os Estados Unidos e o México.

A Operação Interdição foi um fracasso devido à impossibilidade de controlar toda a fronteira através da disposição física. Apesar de terem sido destacados dois mil agentes aduaneiros, não foram alcançados resultados efectivos (ver Reid, 2022). No entanto, o apoio público e político deu lugar a novas acções que abriram a porta a novos tipos de procedimentos. Foi o caso do Comprehensive Drug Abuse Prevention and Control Act (CDAPC Act) de 1970, adotado para reforçar o controlo dos Estados Unidos, entre outras coisas, ao longo da fronteira sul.

A Operação Interdição e a Lei CDAPC representam os marcos em que se basearam os seus discursos de 1971. De facto, estas acções desencadearam uma série de procedimentos governamentais adicionais para intensificar a guerra contra a droga. Uma indicação da forma como o Presidente Nixon pretendia aumentar estes procedimentos destinados a travar esta ameaça à segurança é visível na seguinte passagem: "Temos agora de reconhecer francamente que os procedimentos deliberados incorporados nos actuais esforços para controlar o abuso de drogas não são suficientes em si mesmos. O problema assumiu as dimensões de uma emergência nacional" (Departamento de Defesa dos EUA, 2017, p. 3). Foi assim que conseguiu obter apoio bipartidário para enfrentar esta nova e aparentemente devastadora ameaça à segurança.

Para ser mais preciso, as medidas legislativas mais importantes adoptadas desde os dois discursos analisados nesta secção foram a fundação, por Ordem Executiva, do Gabinete de Ação Especial para a Prevenção do Abuso de Drogas em 1971, a extensão da Lei de Reabilitação de Toxicodependentes de 1966 em 1971, a organização da Lei de Assistência à Segurança Internacional de 1971 juntamente com a Lei de Desenvolvimento Internacional e Assistência Humanitária de 1971, a criação do Gabinete de Aplicação da Lei sobre o Abuso de Drogas em 1972 e a criação da Administração de Combate à Droga (DEA) em 1973.

É importante sublinhar que tais acções só foram possíveis com um amplo apoio político. O Presidente estava ciente desta característica, uma vez que, ao longo da sua conferência de imprensa, se referiu repetidamente ao apoio bipartidário às suas acções. Este é um aspeto importante quando se analisa a teoria da securitização, pois realça o poder que a aceitação geral confere à elite que enquadra a ameaça à segurança. Este poder permite à elite tomar medidas extraordinárias num curto espaço de tempo, algo que entra em conflito com os longos procedimentos burocráticos que são ultrapassados em tais situações.

Para além do apoio político, Nixon conseguiu fazer com que a sociedade aceitasse a ameaça que conseguiu enquadrar. Fê-lo sublinhando como todos os membros da sociedade americana eram afectados pela ameaça da droga. Ao afirmar que "em 1960, houve menos de 200 mortes por narcóticos na cidade de Nova Iorque. Em 1970, o número tinha aumentado para mais de 1 000" (Departamento de Defesa dos EUA, 2017, p. 2), Nixon conseguiu estabelecer uma relação vertical entre o autor do ato de fala e o seu público. O argumento apresentado pelo Presidente dos EUA é que a população média dos

EUA estava a cair nas drogas. Trata-se de um argumento convincente com o qual as pessoas se podiam identificar, uma vez que estava a acontecer perto delas. O esforço para convencer o seu público exemplifica outro aspeto fundamental mencionado na teoria da securitização. Ou seja, revela a forma como os membros da elite tentam criar uma questão e obter reconhecimento entre um público alargado.

Uma situação semelhante é descrita no mesmo discurso em que Nixon tentou apelar a uma resposta comunitária, explorando os sentimentos individuais. A frase em questão é: "Para derrotar este inimigo, que está a causar tanta preocupação, e com razão, a tantas famílias americanas, será fornecido dinheiro" (Departamento de Defesa dos EUA, 2017, p. 1). O que o presidente dos EUA procurou fazer aqui foi garantir o favor final do seu público. É através de declarações como esta que a legitimação é alcançada e deve, portanto, ser vista como uma parte inerente do processo de enquadramento da ameaça na securitização.

O processo de legitimação era necessário para tomar medidas nas fronteiras dos EUA e para além delas. Como afirmou: "Nenhum ataque sério ao nosso problema interno de drogas pode ignorar as implicações internacionais de tal esforço, nem o esforço interno pode ser bem-sucedido sem atacar o problema num plano internacional" e, em seguida, "estou a iniciar uma escalada global dos nossos programas existentes de controlo do tráfico de estupefacientes" (Departamento de Defesa dos EUA, 2017, p. 11). Estas acções visavam principalmente os traficantes de droga em solo americano. Nas palavras do presidente: "acabar com o tráfico de droga, atingindo os produtores de droga ilegal [...] e o tráfico dessas drogas através das nossas fronteiras" (p. 4). Por outras palavras, Nixon enquadrou os traficantes de droga estrangeiros como uma ameaça, alargando o âmbito de quem era a causa principal que produzia a ameaça que punha em perigo a segurança dos EUA. Estas eram questões-chave que iriam doravante moldar as relações externas do país, especialmente com os estados abaixo da sua fronteira sul.

Os discursos utilizados para esta análise do discurso foram úteis para identificar os padrões propostos pela teoria da securitização. Ao dirigir-se ao Congresso e ao público americano em discursos subsequentes, o Presidente Nixon conseguiu revigorar a transformação do problema da droga numa questão de segurança persistente. Desta forma, os marcadores da teoria da securitização ajudaram a traçar a evolução de um problema criminal e de saúde pública relativamente convencional para um problema que exigia mudanças políticas substanciais. A fim de desenvolver o processo de securitização empreendido pelos EUA para introduzir mecanismos virtuais de aplicação da lei na sua fronteira territorial sul entre 1969 e 1974, a secção seguinte examina uma série de fontes secundárias que foram escritas sobre este tópico.

5.1.2 A virtualização da fronteira durante a administração Nixon

A primeira medida concreta para combater o contrabando de droga do México para os EUA foi tomada pelo Presidente Richard Nixon em 1969 com a Operação Intercetar. De acordo com Grillo (2013), esta operação consistia em revistar "todos os veículos ou peões que atravessassem a fronteira sul, enquanto os militares instalavam unidades móveis de radar entre postos" (p. 256). Este plano acabou por ser um fiasco, pois rapidamente se tornou claro que um controlo exaustivo no terreno era utópico. O pessoal no terreno, por si só, não era capaz de selar toda a fronteira com o México. Como observou Ghaffaray (2019), a fronteira que separa os Estados Unidos do México era demasiado larga e a sua

orografia demasiado injustificada para ser vedada na sua totalidade. Por esta razão, a Operação Intercetar, que custou 30 milhões de dólares, durou apenas 17 dias.

No entanto, Mendoza (2023) observou que Nixon decidiu fortificar a fronteira com uma vedação virtual, e não física, a fim de obter melhores resultados na redução dos fluxos de droga. Ou seja, notando que fechar fisicamente a fronteira por si só era quixotesco, Nixon investiu na estrutura de controlo fronteiriço existente para melhorar tecnologicamente a securitização da fronteira. Além disso, Koslowski (2019) explicou que, nessa altura, o governo dos EUA instalou sensores de movimento, infravermelhos, sísmicos e magnéticos capazes de detetar tanto o movimento como o calor a uma distância de 50 a 250 pés. A justificação utilizada por Nixon para legitimar o investimento em mecanismos digitais foi a proteção da fronteira comum com o México: a guerra contra a droga.

A necessidade de Nixon coincidia com os interesses das empresas militares americanas de alta tecnologia. O fim iminente da guerra do Vietname obrigou estas empresas a diversificarem-se e a começarem a investir em sistemas de apoio às forças armadas americanas. Para o fazer, tiveram de convencer o governo dos EUA a continuar a investir em diferentes tipos de despesas militares, ou seja, uma defesa a ser conduzida a nível interno e não apenas a nível internacional. Assim, a partir do final dos anos 60, várias empresas de investigação e desenvolvimento contratadas pelos EUA para apoiar a intervenção militar no Vietname conseguiram assinar contratos federais.

A Sylvania Electronics, por exemplo, foi bem sucedida. Mais concretamente, vendeu os seus sensores terrestres de deteção remota de movimentos no solo ao governo americano em 1970. Este foi um evento pioneiro, pois simbolizou a primeira aplicação de tecnologias virtuais utilizadas para monitorizar a fronteira sul dos Estados Unidos. Grandin (2019) especificou que estes sensores foram industrializados no âmbito do plano do Secretário da Defesa Robert McNamara para construir uma vedação virtual e física que separasse o Vietname do Norte do Vietname do Sul e foram utilizados para detetar movimentos de tropas e camiões ao longo do trilho de Ho Chi Minh. A principal função destes sensores era detetar a atividade sísmica causada por pessoas ou camiões que passavam perto dos sensores e moviam o solo (Rosenau, 2001, pp. 11-12). Esta tecnologia era também útil para detetar movimentos através e nas proximidades da fronteira dos EUA, razão pela qual foi implementada durante o mandato de Nixon.

Outro elemento tecnológico utilizado pela primeira vez durante a Guerra do Vietname e mais tarde na fronteira entre os EUA e o México foram os drones. Estes drones, de acordo com Novak (2015), eram conhecidos como RPVs (Remotely Piloted Vehicles) - enquanto atualmente são conhecidos como Unmanned Aerial Vehicles (UAVs) - e eram utilizados para analisar a área a partir de cima. Descrevendo a fronteira mexicana de 1972, Novak explicou que:

Os drones *QU-22b* da Força Aérea dos EUA e os drones *drone* - que eram excedentários no Vietname graças à introdução de drones mais sofisticados - foram devolvidos aos Estados Unidos, onde [voaram] sobre a fronteira para monitorizar sensores e transmitir dados para pontos de controlo centrais (Novak, 2015).

Com o advento dos drones, foi criado um centro de vigilância para receber as informações recolhidas pelos UAVs. Barkan (1972, p. 1) racionalizou que esses UAVs

sobrevoavam trechos remotos da fronteira para retransmitir sinais de centenas de sensores terrestres que eram então enviados para o chamado Centro de Vigilância de Infiltração, onde enormes computadores diagnosticavam os dados.

5.2 Resultados e efeitos aplicados da titularização da Nixon

A Guerra do Vietname representa um marco para a securitização virtual da fronteira entre os Estados Unidos e o México durante a presidência de Nixon. De facto, houve uma clara mudança na aplicação de tecnologias de guerra às fronteiras internas dos Estados Unidos, resultando numa virtualização da fronteira. Estes desenvolvimentos foram úteis à administração Nixon para alimentar o desejo de travar a guerra contra a droga. Consequentemente, esta foi acompanhada por um empenho político crescente em selar a fronteira (), um termo normalmente utilizado em missões militares, mas pela primeira vez relacionado com a fronteira dos EUA na altura (Lee, 2005), uma vez que um dos principais objectivos era impedir a entrada de traficantes de droga na fronteira sul dos Estados Unidos.

Embora os sistemas de vigilância introduzidos pela Administração Nixon nem sempre tenham funcionado - como Barkan (1972, p. 2) salientou implacavelmente, "são incapazes de distinguir o amigo do inimigo" - foram inegavelmente um passo importante no controlo das fronteiras dos EUA. Esta inovação provou ser uma pedra angular para quase todos os presidentes subsequentes no que diz respeito à gestão da fronteira sul dos EUA. O facto de uma nova tendência tão importante se basear num ato performativo, tal como descrito pela teoria da securitização, explica a importância da criação de ameaças à segurança na percepção do público para a promoção de medidas de segurança.

Tal como tinha sido debatido décadas após a Guerra contra a Droga, não existia, de facto, uma ameaça de droga, ou pelo menos não na medida em que o Presidente Nixon começou por referir. John Ehrlichman, então Assistente do Presidente para os Assuntos Internos de Nixon, admitiu que a Administração estava a mentir sobre a ameaça da droga para permitir movimentos políticos e militares (ver López, 2016). Em todo o caso, existia um verdadeiro problema de droga entre os militares norte-americanos no estrangeiro e longe do solo dos EUA (ver Vulliamy, 2011).

A adoção de uma abordagem baseada na segurança da fronteira entre os Estados Unidos e o México, iniciada por Nixon, tem consequências conexas. É necessário considerar a literatura sobre o uso de alegorias como um meio de polarização. Estas, de facto, elucidam a relação entre a securitização, os actos de fala e a criação de lutas sociais no âmbito do processo mais amplo de justificação da vigilância das fronteiras e dos poderes de emergência. É o caso de Kruglanski (2007), que se centrou na ideia de metáforas para ilustrar como a linguagem é capaz de enquadrar as ameaças, determinando o processo de resposta política. O discurso do "inimigo número um" de Nixon coincide com a metáfora de guerra de Kruglanski. Para ser mais exato, as metáforas de guerra de Nixon espelham as do discurso de Kruglanski (2007) sobre o terrorismo. Isto sugere que a securitização da fronteira dos EUA tem sido utilizada mesmo em tempos mais recentes. Em ambos os casos, a resposta totalizante foi possível através da legitimação de medidas de emergência como a vigilância das fronteiras.

As desvantagens da utilização desta abordagem no processo de securitização dos EUA residem nos seus efeitos polarizadores e radicalizadores a longo prazo. Por exemplo,

Moyano *et al.* (2016) criticaram o processo de securitização da era Bush (a Guerra ao Terror) causado pelo ato terrorista de 11 de setembro. Na sua opinião, a sociedade norte-americana teria beneficiado mais com uma narrativa menos polarizadora que evitasse as disjunções sociais que afectam a atual divisão social. O mesmo se pode dizer da abordagem de Nixon à Guerra contra a Droga. De facto, seguindo esta ideia, enquadrar a questão como uma guerra e não como um desafio humano ofuscou os problemas associados de saúde pública e de desenvolvimento comunitário que assolavam os Estados Unidos. Teria sido aconselhável, portanto, adaptar a concepção dos seus actos discursivos. A longo prazo, teria sido mais rentável optar por uma resposta mais holística. Estas deveriam ter sido baseadas numa abordagem multidisciplinar para evitar os retrocessos criados pelos processos de securitização que apenas consideram uma questão.

6. DEBATE

Este trabalho procurou responder às seguintes questões de investigação: Como é que a Guerra contra a Droga durante a Administração Nixon contribuiu para a transição do controlo fronteiriço físico ao longo da fronteira sul para mecanismos virtuais de aplicação da lei? Para encontrar uma resposta a esta questão, esta investigação recorreu aos principais princípios que constituem a teoria da securitização. Estes princípios foram utilizados como indicadores para efetuar uma análise do discurso de dois discursos proferidos por Nixon em que este declarou oficialmente a sua Guerra contra a Droga. O resultado desta análise é que o Presidente Nixon participou ativamente no enquadramento de uma ameaça à segurança proposta ao seu público e à sua audiência política como prejudicial à segurança nacional de todo o país. Graças à aceitação da narrativa por parte da audiência, foram tomadas medidas extraordinárias para impedir a entrada de drogas nos Estados. Entre essas medidas, foi possível identificar a introdução de mecanismos virtuais de fiscalização.

Investigações anteriores apontaram para a importância da fronteira virtual na definição da fronteira sul dos EUA. Heyman (2008) salientou a forma como os muros e as vedações são reforçados pelo aspeto virtual que define o lado coercivo da política de imigração dos EUA. Uma ideia avançada por Amoores *et al.* (2008, pp. 99-100) ao enumerarem o conjunto de tecnologias utilizadas para ajudar a Patrulha Fronteiriça dos EUA a classificar, através de algoritmos, o que pode ser considerado uma ameaça e o que não pode. O seu estudo centrou-se, assim, na mudança do papel humano na gestão das fronteiras, bem como na capacidade de controlo dos EUA para além da fronteira física, através do aspeto virtual da sua fronteira. Outro tipo de investigação efectuada sobre a virtualização da fronteira dos EUA estava ligada ao desenvolvimento militar. Tal como sugerido por Adams (2001), os avanços militares na utilização da tecnologia para conduzir a guerra foram utilizados para revigorar a fronteira inteligente que separa os EUA do México, a fim de garantir um controlo ótimo.

Tendo em conta esta investigação existente, tornou-se evidente uma lacuna na literatura. Ou seja, embora a securitização, a virtualização e a militarização da fronteira ao longo da fronteira sul dos EUA tenham sido estudadas, o início desta transformação não foi devidamente considerado. O objetivo deste trabalho foi precisamente preencher esta lacuna. Após a realização desta investigação, tornou-se claro que a presidência de Nixon provou ser inovadora para a história da gestão das fronteiras nos Estados Unidos. De facto, foi a primeira vez que os Estados implementaram elementos tecnológicos - como sensores terrestres e as primeiras versões de veículos aéreos não tripulados - para

monitorizar a fronteira entre os Estados Unidos e o México. Ao preencher esta lacuna no debate académico sobre as origens da fronteira inteligente para os Estados, é possível avançar ainda mais na investigação e comparação das fronteiras numa perspetiva de estudos de segurança. Além disso, ao testar a teoria da securitização para realizar com sucesso uma análise do discurso empreendida pelas elites políticas para enquadrar as necessidades de segurança, as conclusões desta investigação também podem ser aplicadas a outros casos. Por exemplo, seria possível aplicar esta investigação a casos semelhantes, como a fronteira espanhola partilhada com Marrocos. A teoria da securitização utilizada neste estudo poderia esclarecer como e quando os mecanismos de fronteira virtual foram introduzidos no regime fronteiriço espanhol.

No entanto, também é necessário mencionar as limitações deste trabalho. Embora a escolha de realizar um estudo de caso único tenha sido necessária para fornecer uma descrição exacta do papel de Nixon na promoção da virtualização da fronteira EUA-México, um estudo comparativo poderia ter proporcionado uma compreensão abrangente das fronteiras em geral. Do mesmo modo, a utilização de uma abordagem de método misto para efetuar este estudo também poderia aumentar a validade das conclusões. A integração de uma perspetiva quantitativa na abordagem qualitativa privilegiada nesta investigação poderia fornecer informações importantes para localizar as partes das fronteiras mais fortificadas em relação ao processo de virtualização.

As limitações deste trabalho representam, no entanto, uma oportunidade para estimular mais investigação sobre este tema. Comparar os resultados deste estudo com outros casos em que se registaram progressos significativos na virtualização das fronteiras como parte de um processo de fortificação mais geral. As cidades autónomas espanholas de Ceuta e Melilla, por exemplo, poderiam beneficiar deste tipo de análise. Compreender o seu processo de fortificação das fronteiras desde a sua adesão ao Espaço Schengen forneceria informações significativas sobre a forma como a gestão das fronteiras mudou devido às práticas de fronteiras virtuais. Determinar se o início desta digitalização foi complementado pelo exemplo fornecido anteriormente pelos EUA poderia ajudar a conceber as fronteiras de Ceuta e Melilla de uma forma mais abrangente. Além disso, a aplicação da teoria da securitização a estes casos específicos poderia revelar a dupla importância da narrativa nacional que justifica esta mudança no regime fronteiriço, juntamente com a narrativa implementada pela União Europeia. Desta forma, seria possível analisar a ideia da Fortaleza Europa do ponto de vista da securitização virtual.

De um modo geral, as tentativas de Nixon para combater o contrabando de droga através da fronteira sul dos EUA lançaram as bases para décadas de política fronteiriça entre os EUA e o México. A importância desta mudança no regime fronteiriço é visível no atual *modus operandi* da Patrulha de Fronteira. Manter o controlo da fronteira sul seria virtualmente impossível sem as tecnologias militares dos EUA utilizadas no Vietname e introduzidas na fronteira nacional sob Nixon. Ao traçar as origens do controlo virtual das fronteiras até à Guerra contra a Droga de Nixon, este estudo revela como a política de segurança pode transformar discretamente a própria arquitetura das fronteiras de uma nação.

REFERÊNCIAS BIBLIOGRÁFICAS

- Adams, J. (2001). Virtual defence. *Foreign Affairs*, 80(3), 98-112.
- Amoore, L., Marmura, S., & Salter, M. B. (2008). Fronteiras e mobilidades inteligentes: Zoned spaces, enclosures. *Surveillance & Society*, 5(2).
- Armstrong, W. G. (1992). Punição, vigilância e disciplina no Paraíso Perdido. *Studies in English Literature, 1500-1900*, 32(1), 91-109. <https://doi.org/10.2307/450942>
- Barkan, R. (1972, 18 de fevereiro). Eles observam-nos, através das paredes, na escuridão da noite, enquanto caminhamos, e isso vem do Vietname. *Free Press*.
- Dafoe, A. (2015). Sobre o Determinismo Tecnológico: Uma Tipologia, Condições de Âmbito e um Mecanismo. *Science, Technology and Human Values*, 40(6), 1047-1076. <http://www.jstor.org/stable/43671266>
- Ghaffary, S. (2019, 16 de maio). A parede "mais inteligente": como drones, sensores e IA são a patrulhar a fronteira. *Vox*.
- Grandin, G. (2019, 9 de fevereiro). Como é que os Estados Unidos construíram o muro da fronteira. *The Intercept*.
- Grillo, I. (2013). Os cartéis mexicanos: um século desafiando a política de drogas dos EUA. *The Brown Journal of World Affairs*, 20(1), 253-265. <http://www.jstor.org/stable/24590897>
- Heyman, J. McC. (2008). Constructing a Virtual Wall: Race and Citizenship in U.S.-Mexico Border Policing [Construindo um Muro Virtual: Raça e Cidadania no Policiamento da Fronteira EUA-México]. *Journal of the Southwest*, 50(3), 305-333.
- Kerr, D. (1999). Decapitando o Rei e Entronizando o Mercado: Uma Crítica da Governamentalidade Foucaultiana. *Science & Society*, 63(2), 173-202.
- Koslowski, R. K. (2019, 29 de maio). *Reformas da imigração e segurança das fronteiras. fronteiras*. Artigos. <https://items.ssrc.org/border-battles/immigration-reforms-and-technologies-of-border-security/>
- Kruglanski, A. W., Crenshaw, M., Post, J. M., & Victoroff, J. (2007). What Should This Fight Be Called? Metaphors of Counterterrorism and Their Implications [Metáforas do Contraterrorismo e suas Implicações]. *Psychological Science in the Public Interest*, 8(3), 97-133. <http://www.jstor.org/stable/40062365>
- Lee, J. (2005, 31 de agosto). James H. Scheuer, congressista de Nova Iorque com 13 mandatos, morreu aos 85 anos. *The New York Times*.
- Lemke, T. (2015). *Foucault, governamentalidade e crítica*. Routledge.

- López, G. (2016, 22 de março). *Funcionário de Nixon: A verdadeira razão para a guerra contra as drogas era criminalizar negros e hippies*. Vox. <https://www.vox.com/2016/3/22/11278760/war-on-drogas-racismo-nixon>
- Lynch, M. (2008). *Ideias e perspectivas*. Em *The Handbook of Science and Technology Studies* editado por Hackett, E. J., Amsterdamska, O., e Wajcman, J., 9-11. Cambridge, MA: MIT Press
- Mendoza, M. E. (2023, 30 de outubro). *A história do muro da fronteira entre os EUA e o México*. Time. <https://time.com/6324599/bidens-trump-history-border-wall/>
- Moyano, M., Bermúdez, M. I., & Ramírez, A. (2016). Psicologia positiva para enfrentar a radicalização e o terrorismo? Uma análise do discurso de Obama no Cairo. *Escritos De Psicología - Escritos Psicológicos*, 9(3), 53-58. <https://doi.org/10.24310/espsiescpsi.v9i3.13219>
- Nail, T. (2016). *Frontier theory*. Oxford University Press.
- Novak, M. (2015, 24 de setembro). Como a Guerra do Vietname trouxe a vigilância de alta tecnologia para os Estados Unidos. Gizmodo.
- Otukoya, T. A. (2024). A teoria da securitização. *Revista Internacional de Ciência e Investigação*, 11(1), 1747-1755. <https://doi.org/10.30574/ijsra.2024.11.1.0225>
- Paden, R. (1984). Surveillance and Torture: Foucault and Orwell on the Methods of Discipline (Vigilância e Tortura: Foucault e Orwell sobre os Métodos de Disciplina). *Social Theory and Practice*, 10(3), 261-271.
- Reid, Justin M. "'An Exercise in International Extortion': Operation 'Intercept' and Nixon's 1969's War on Drugs". Tese de mestrado, Chapman University, 2022. <https://doi.org/10.36837/chapman.000412>
- Sharma, V. (2023). Uma análise da "Teoria das Fronteiras" de Thomas Nail. Nova Zelândia *Journal of Asian Studies*.
- Smith, M. R., & Marx, L. (Eds.) (1994). *Does technology drive history? O dilema do determinismo tecnológico*. Mit Press.
- Timmons, P. (2017). O muro de Trump na fronteira de Nixon: como a Operação Intercetação lançou as bases para décadas de política de fronteira EUA-México, incluindo o muro de Donald Trump. *NACLA Report on the Americas*, 49(1), 15-24. <https://doi.org/10.1080/10714839.2017.1298238>. <https://doi.org/10.1080/10714839.2017.1298238>
- Toshkov, D. (2016). *Research design in political science*. Basingstoke: Palgrave Macmillan.
- Trist, N., Cuevas, L., Couto, B., & Atristain, M. (2022). O Tratado de Guadalupe Hidalgo. Em GM Joseph e TJ Henderson (Eds.), *O leitor do México: história, cultura,*

política (pp. 599-603). Duke University Press.
<https://doi.org/10.2307/j.ctv2rr3g8m.96>

Alfândegas e Proteção das Fronteiras dos EUA (2019). *Sabia que... Obeliscos com séculos de idade marcam a linha de fronteira entre os EUA e o México....* Alfândega e Proteção das Fronteiras dos EUA. <https://www.cbp.gov/about/history/did-you-know/obelisk>

Departamento de Defesa dos Estados Unidos (2017). *41 Nixon Remarks Intensified Program for Drug Abuse*. Governo dos EUA.

Vulliamy, E. (2011, 23 de julho). *A "Guerra às Drogas" de Nixon começou há 40 anos e a batalha continua.* The Guardian.
<https://www.theguardian.com/society/2011/jul/24/war-on-drugs-40-years>

Wæver, O. (1995). Securitization and Desecuritization. Em R. D. Lipschutz (Ed.), *On Security* (pp. 46-87). Columbia University Press.



Artigo de investigação

VIOLÊNCIA SEXUAL PERPETRADA POR DESCONHECIDOS EM MADRID E BARCELONA: UMA ANÁLISE SITUACIONAL

Tradução para o português com ajuda de IA (DeepL)

Francisco Pérez Fernández

Doutor em Filosofia e Ciências da Educação, Professor Associado (Psicologia Criminal, Psicologia da Personalidade e História da Psicologia), Departamentos de Psicologia e de Criminologia e Segurança, Hospitais HM Faculdade de Ciências da Saúde, Universidade Camilo José Cela.

fperez@ucjc.edu

ORCID ID: 0000-0002-3039-2397

Google Scholar: https://scholar.google.es/citations?hl=es&user=O_7qrwgAAAAJ

Heriberto Janosch

Doutor em Ciências Jurídico-Económicas,
Professor de História da Psicologia e de Bases Biológicas do Comportamento, Faculdade de Saúde,
Universidade UNIE

heriberto.janosch@universidadunie.com

ORCID ID: 0000-0002-0188-2434

Google Scholar: <https://scholar.google.com/citations?user=uA4iKy0AAAAJ>

Enrique López López

Magistrado da Audiência Nacional de Espanha.
Professor de Direito Constitucional e Direito Processual Penal, Faculdade de Ciências Jurídicas e
Relações Internacionais, Universidade UNIE
enrique.lopezl@universidadunie.com

Francisco López-Muñoz

Doutor em Medicina e Cirurgia e Doutor em Língua e Literatura Espanhola, Professor de Farmacologia
e Vice-Reitor de Investigação e Ciência da Faculdade HM Hospitais de Ciências da Saúde da
Universidade Camilo José Cela.

flopez@ucjc.edu

ORCID ID: 0000-0002-5188-6038

Google Scholar: <https://scholar.google.es/citations?user=IbuwtWgAAAAJ&hl=es>

Recebido em 28/03/2025

Aceite em 23/05/2025

Publicado em 27/06/2025

Citação recomendada: Pérez, F, Janosch, H, López, E e López, F (2025). Violência sexual por desconhecidos em Madrid e Barcelona: uma análise situacional. *Revista Logos Guardia Civil*, 3(2), p.p. 171-196.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

VIOLÊNCIA SEXUAL PERPETRADA POR DESCONHECIDOS EM MADRID E BARCELONA: UMA ANÁLISE SITUACIONAL

Resumo: INTRODUÇÃO. 2. HIPÓTESE. 3. METODOLOGIA. 4. RESULTADOS. 5. DISCUSSÃO. 6. CONCLUSÕES. 7.

Resumo: As agressões sexuais, enquanto crimes de especial vitimização e importância mediática, suscitam grande alarme, preocupação e interesse público. Por conseguinte, encontram-se frequentemente no epicentro do debate geral sobre política criminal. Em consequência, as agressões sexuais e os seus protagonistas - agressor e vítima - nem sempre são adequadamente analisados, tratados e compreendidos fora dos ambientes criminológicos, policiais e jurídicos. Do mesmo modo, a própria investigação criminológica, bem como os desenvolvimentos legislativos, jurídicos e penitenciários ligados ao tema - necessariamente polémicos - tendem, muitas vezes, a esbater-se em generalidades teóricas difíceis de confrontar e mesmo de enquadrar com factos e casos particulares que, quando estudados em pormenor, parecem impossíveis de enquadrar nos quadros explicativos gerais disponíveis. O presente estudo, que se baseia na abordagem proporcionada pela Teoria da Ação Situacional (TAS), proposta por Wikström e seus colaboradores, e recorre à análise qualitativa e quantitativa de sentenças judiciais proferidas nas províncias de Madrid e Barcelona, pretende mostrar como os ecossistemas penais em que os crimes são cometidos modificam substancialmente o seu curso, bem como as acções do agressor e da sua vítima. Um facto que pode ser extremamente útil como ferramenta de investigação policial e de análise comportamental, bem como para a compreensão de eventos criminogénéticos e dinâmicas criminais específicas.

Resumen: Las agresiones sexuales, en tanto que delitos de especial significación victimal y mediática, suscitan gran alarma, preocupación e interés públicos. En consecuencia, suelen formar parte del epicentro del debate general en torno a las políticas criminales. Ello motiva que las agresiones sexuales y sus protagonistas -agresor y víctima- no siempre sean adecuadamente analizados, tratados y entendidos fuera de los entornos criminológicos, policiales y jurídicos. Del mismo modo, la propia investigación criminológica, así como el devenir legislativo, jurídico y penitenciario vinculados al tema -necesariamente controvertido-, tienden a menudo a difuminarse en generalidades teóricas que cuesta confrontar e incluso encajar con hechos y casos particulares que, al estudiarse en detalle, parece imposible de encajar en los marcos explicativos generales de que se dispone. El presente estudio, que se realiza partiendo del enfoque aportado por la Teoría de la Acción Situacional (TAS), propuesta por Wikström y sus colaboradores, y se vale del análisis cualitativo y cuantitativo de sentencias judiciales emitidas en las provincias de Madrid y Barcelona, pretende mostrar cómo los ecosistemas criminales en que se cometen los delitos, modifican sustancialmente su curso, así como las acciones del agresor y su víctima. Un hecho que puede ser extremadamente útil como herramienta para la investigación policial y el análisis de conducta, así como para la comprensión de eventos criminogénéticos y dinámicas criminales específicas.

Palavras-chave: Agressão Sexual, Teoria da Ação Situacional, Escala Multidimensional, Análise do Comportamento.

Palabras clave: Agresión Sexual, Teoría de la Acción Situacional, Escalamiento Multidimensional, Análisis de Conducta.

1. INTRODUÇÃO

As agressões sexuais são uma fonte de sofrimento para as vítimas. Esta situação é agravada nos casos que, por razões peculiares, se tornam particularmente "famosos" e despertam o interesse da opinião pública. O facto é que as agressões sexuais, muitas vezes altamente publicitadas, provocam grande alarme e debate social, o que geralmente desencadeia investigações e julgamentos particularmente mediáticos que têm um forte impacto nas vítimas através da vitimização secundária e *ex post attendentes*¹ (Gutiérrez de Piñeres, Coronel e Pérez, 2009; Domínguez Vela, 2016). Para fornecer alguns dados para reflexão, convém recordar que, de acordo com o Anuário Estatístico do Ministério do Interior de Espanha, em 2022, 19.013 crimes contra a liberdade sexual foram "conhecidos" pelas Forças e Corpos de Segurança do Estado (FCSE) - fala-se de denúncias e investigações -, dos quais 11.426 foram abusos/agressões sexuais e, destes, 4.270 foram abusos/agressões sexuais com penetração². Uma elevada percentagem destas agressões/abusos ocorreu em estabelecimentos comerciais, habitações e outros espaços anexos, como garagens ou arrecadações, sendo uma das modalidades mais frequentes deste tipo de crime aquela em que o agressor sexual, geralmente um homem agindo sozinho, ataca uma mulher no hall de entrada de um edifício residencial, ou na garagem, pelo que é vulgarmente conhecido como "portalero" (Janosch González, Pérez-Fernández e Soto Castro, 2020).

Seja como for, a "cifra cinzenta" das estatísticas reflecte a sinistra evidência policial, de vitimização e judicial que está subjacente a este problema: o esclarecimento de agressões sexuais cometidas por indivíduos desconhecidos das vítimas é mais complexo do que naqueles casos em que existe algum tipo de ligação entre vítima e agressor que facilite aos investigadores do FCSE a identificação positiva do agressor e, se necessário, a obtenção de indícios que possam ser utilizados como prova em tribunal (Corovic, Christianson e Bergman, 2012; Janosch, Pérez-Fernández e Herrero, 2025). Há que ter em conta que as dinâmicas cognitivo-comportamentais destes indivíduos tendem a funcionar através de um processo de escalada, o que implica que, em relação à sua potencial perigosidade, é muito possível que exista um viés de serialidade - ou, pelo menos, de repetitividade - que os leve a cometer mais do que uma agressão sexual ao longo da sua carreira criminosa, caso não sejam identificados e detidos (Pueyo e Redondo Illescas, 2007). Especialmente porque, em vez de uma ligação direta a perturbações diagnosticáveis mais ou menos graves, nesta classe de agressores parece ser impulsionada pela influência de uma amálgama complexa de elementos socioculturais, stressores de vida e estruturas de personalidade (Arqué-Valle et al., 2024).

Por outro lado, e para desenvolver esta última ideia, é sabido que o contexto - ambiente material e humano - em que o delinquentes actua modifica o seu comportamento,

¹ Estes dois tipos de vitimação são frequentemente confundidos. A vitimação secundária diz respeito aos custos pessoais e psicológicos para a vítima pelo facto de estar mais ou menos constantemente exposta a situações que a fazem reviver (ou recordar) os danos sofridos repetidamente (Kühne, 1986). A vitimação *ex-post* - também designada por vitimação de "quarto nível" - é desencadeada quando a pessoa experimenta desesperança e desamparo depois de não ter recebido a ajuda esperada por parte das instituições e profissionais em que confiava (como a polícia, a saúde, a administração, a justiça) e de quem não recebe o apoio moral e material esperado (Triviño, Winberg e Moral, 2021).

² No total, foram resolvidos 14.555 crimes contra a liberdade sexual, contando todos os tipos de crimes contra a liberdade sexual, o que resulta numa "cifra cinzenta" - crime investigado mas não resolvido - de 4.518 queixas. Em termos de abuso/agressão com penetração, o número de casos não resolvidos em 2022 era de 860 (Ministério do Interior, 2023).

pelo que estratégias e recursos que podem ser perfeitamente úteis num determinado local não têm necessariamente o mesmo valor de aplicabilidade num ecossistema criminoso-delinquente diferente. Wikström, perante esta contingência, desenvolveu a chamada Teoria da Ação Situacional da Causalidade do Crime (ou CAS), cujas propostas fundacionais surgiram entre 2004 e 2006 (Serrano Maíllo, 2017). Aí se procurou integrar, no quadro de uma teoria da ação adequada, as principais conquistas das formulações teóricas e da investigação em criminologia, bem como os conhecimentos teóricos e empíricos das ciências sociais e comportamentais em geral. Isto porque os correlatos da criminalidade são bastante conhecidos, mas há pouco consenso sobre as causas da criminalidade, que se apresentam como uma mistura confusa de elementos a que cada investigador atribui maior ou menor importância em função dos seus interesses. Isto explica a inflação de teorias - e as contradições internas - que afectam os estudos criminológicos (Pérez-Fernández, Janosch e Popiuc, 2023).

Em suma, a TAS afirma que os actos criminosos podem ser explicados como processos - mecanismos sistémicos e interactivos, mas não determinísticos - que mobilizam "acções" que acabam por transgredir regras de conduta formais ou informais (Wikström, et al., 2012). Tratar-se-ia, assim, de um subconjunto de comportamentos incluídos no conjunto mais geral de *actos que violam regras morais de conduta*. Embora estas construções de conduta moral não estejam especificadas em nenhuma lei e, portanto, nem todas sejam crimes per se, poderiam responder aos mesmos mecanismos que mobilizam os crimes em sentido jurídico (Janosch González, 2013). Por outras palavras, a TAS define o crime como um ato que viola alguma regra de conduta estabelecida por lei - inserida no código penal de cada Estado - e que pode ser analisada em termos de *ação moral*. A ação moral, por sua vez, seria entendida como uma conduta orientada por regras que estabelecem o que, em determinadas circunstâncias - ou situações - específicas, seria certo ou errado fazer (Wikström e Treiber, 2016).

Definir o crime nestes termos, como um ato que viola uma regra de conduta moral que se concretiza sob a forma de leis, tem a vantagem de poder ser aplicado a qualquer tipo de crime, em qualquer lugar e em qualquer momento. Assim, o que é definido é um ato de violação de uma regra de conduta moral que é especificada sob a forma de alguma lei particular "ali dada". Assim, pode-se argumentar que a TAS é fundamentalmente uma teoria geral da ação moral (Wikström, et al., 2012), uma vez que explicaria todas as acções morais, 2012), pois explicaria todos os tipos de quebra de regras morais em qualquer tempo ou lugar, com ênfase no mecanismo que induz a quebra de regras morais, e não no conteúdo da regra moral desobedecida como variável e sujeito a modificações constantes de acordo com as variações da lei positiva particular em um espaço-tempo específico (Pauwels, 2018a; Pauwels, 2018b). O mecanismo causal de percepção e ação estaria presente tanto nos pequenos furtos como nas agressões sexuais ou nos homicídios. Consequência: as políticas criminais, a médio e longo prazo, seriam mais bem-sucedidas se visassem a educação em conformidade com a regra moral prevalecente, e não a punição ou o mero controlo (Pérez-Fernández, Janosch e Popiuc, 2023; Janosch, Pérez-Fernández, Popiuc e López-Muñoz, 2024).

Em última análise, é a interação entre a propensão para o crime de uma determinada pessoa e as características criminogénicas do contexto que desencadeará o processo que conduzirá - ou não - ao ato criminoso propriamente dito. A propensão para o crime dependerá dos padrões morais e da capacidade de autocontrolo da pessoa - tendo em conta que esta capacidade pode estar diminuída pelo consumo de álcool ou de drogas, ou por

stress intenso com desequilíbrio emocional. Estas características criminogénicas do cenário, por sua vez, dependerão do chamado "ambiente moral" - aquele que é percebido pelo indivíduo e não o real - e da existência ou não de factores dissuasores, que incentivem ou desincentivem a violação de regras (Wikström, et al., 2012). O corolário de tudo isto, no que a este estudo diz respeito, é claro: o agressor sexual não agirá sempre da mesma forma e com total independência do local onde se encontra, pois a situação geral em que está inserido - que deve ser analisada e compreendida - modificará necessariamente a sua percepção das regras, as suas considerações morais, a sua atenção às leis e restrições e, finalmente, a sua ação delinvente (Pérez-Fernández, Popiuc e López-Muñoz, 2024).

Assim considerado, compreender-se-á que para o CAS, para além de quaisquer ideias discutíveis, a nacionalidade, a ideologia política, a identificação sexual ou a religião de uma pessoa não são, em si mesmas, causas de qualquer tipo de crime, ou pelo menos não devem ser avaliadas como mais importantes do que outras circunstâncias pessoais, como a idade ou o nível de educação, porque na realidade são apenas atributos da pessoa que, além disso, são mutáveis. Tal como não faria sentido dizer que alguém é mais propenso a cometer crimes por ser mais alto, também não faz sentido enfatizar outros atributos pessoais que, além do mais, se enquadrariam na área controversa dos direitos e liberdades individuais. Assim, variáveis como a nacionalidade ou a religião devem ser avaliadas com o mesmo rigor que outras causas contributivas para as diferentes formas de criminalidade reconhecidas na literatura, como a pobreza, o nível de educação, a vivência em ambientes criminogénicos, a falta de oportunidades, o policonsumo, o absentismo, a companhia inadequada, etc. (Pérez-Fernández, Janosch e Popiuc, 2023). Por outras palavras, tal como não faria sentido dizer que uma pessoa comete crimes - ou não comete crimes - por causa da cor do seu cabelo ou do seu peso em quilogramas, também não é coerente argumentar que ela poderia ser levada a cometer crimes simplesmente porque nasceu num determinado país, porque partilha um determinado sentimento ideológico, porque se identifica com um género específico ou porque pratica uma determinada religião (Janosch, Pérez-Fernández e Herrero Roldán, 2024).

1.1. UMA NOTA JURÍDICA NECESSÁRIA

Esta introdução termina recordando algo que é bem conhecido, ou seja, que em Espanha houve alterações relativamente recentes no Código Penal (CP) relativamente aos crimes sexuais, que vieram modificar as diferentes perspectivas existentes relativamente à abordagem policial e judicial do problema. Em primeiro lugar, e em ligação com o modelo TAS acima descrito, implicam uma alteração das contagens estatísticas - que alterarão também os futuros discursos mediáticos - cujos efeitos só serão perceptíveis a médio prazo e, conseqüentemente, abrem novas perspectivas sobre a percepção geral da criminalidade, bem como sobre as políticas reactivas de atuação face à mesma, cujos efeitos ainda estão para vir. Vale, pois, a pena, para antecipar o que está para vir e para contextualizar corretamente os resultados aqui apresentados, fazer um breve enquadramento crítico dessas mudanças.

A LO 10/2022, de 6 de setembro, popularmente conhecida como a *Lei do só sim é sim*, significou uma mudança notável no que respeita à consideração dos crimes contra a liberdade sexual. Este normativo introduziu alterações significativas no CP, nomeadamente na unificação dos crimes de abuso e agressão sexual, na redefinição do consentimento e na modificação das penas associadas. Mas, para além destas novidades

legislativas, gerou também um intenso debate em consequência das reduções de pena que se verificaram: 1205 reduções de pena que incluem 121 saídas da prisão (CGPJ, 2023). A promulgação desta lei foi contextualizada na necessidade de reforçar a proteção da liberdade sexual e de garantir uma resposta abrangente a todas as formas de violência sexual.

Antes da entrada em vigor da LO 10/2022, o Código Penal espanhol estabelecia uma distinção entre abuso sexual e agressão sexual. O abuso referia-se a actos sem violência ou intimidação, enquanto a agressão envolvia o uso de violência ou intimidação. Com a nova lei, esta distinção desaparece. Assim, qualquer ato sexual sem consentimento é considerado agressão sexual, independentemente de ter havido violência ou intimidação. Esta unificação procura reconhecer que qualquer ação sexual não consentida constitui uma agressão à liberdade sexual de uma pessoa.

A lei estabelece que só se entende que existe consentimento quando este tenha sido livremente expresso através de actos que, dadas as circunstâncias do caso, expressem claramente a vontade da pessoa. Esta definição coloca o consentimento no centro das relações sexuais, eliminando interpretações que poderiam justificar condutas não consentidas. Isto implica que qualquer ato sexual não consentido é uma agressão, independentemente de haver ou não violência ou intimidação, porque a ausência de consentimento implica, por si só, uma violência implícita. Embora o consentimento não tenha sido explicitamente definido, tal não significa que a jurisprudência não tenha entendido que esse consentimento era substancial, como elemento, neste caso negativo do tipo, de que o agente actuou: 1) sem o consentimento da pessoa sexualmente agredida; 2) através da existência de um consentimento viciado por circunstâncias concomitantes derivadas da posição do autor do facto, significativamente derivadas do parentesco ou de situação equivalente, ou do domínio que a sua posição em consequência de uma relação de trabalho, de ensino, de superioridade, de ascendência, mesmo em consequência de uma faixa etária relativamente à vítima, pudesse restringir a autodeterminação sexual desta; e 3) que o agente se tenha aproveitado de uma posição de privilégio decorrente da vulnerabilidade ou do estado de inconsciência da vítima³. Estas últimas sequências de atentados à liberdade sexual eram anteriormente classificadas como abuso sexual, enquanto os casos em que o agente agia contra o consentimento da vítima abriam a categoria de agressão sexual, sendo cometidos por meio de violência ou intimidação, característica exigida para tal agressão. No entanto, a concomitância da ausência de consentimento que permeia o título que abarca esses crimes sempre foi necessária, pois são crimes contra a liberdade sexual, que se baseia naturalmente na existência de consentimento na prestação de consentimento para a realização de ações com conteúdo sexual.

A fórmula hoje utilizada pelo legislador é, pois, uma fórmula aberta, e que já era tida em consideração pela jurisprudência, em termos semelhantes, para entender o consentimento como concorrente. A referida fórmula assenta em actos, pelo que "só se entenderá que existe consentimento quando este tiver sido livremente manifestado através de actos que, tendo em conta as circunstâncias do caso, expressem claramente a vontade da pessoa" (LO 10/2022). Por *actos*, entende-se todo o tipo de manifestações ou sinais da pessoa que vai consentir, sejam eles verbais, gestuais ou situacionais, mas que devem ser

3 Ver, por exemplo: STS 3865/2024; SAP A 872/2018.

considerados explícitos. Assim, o consentimento é construído como positivo e concludente, devendo ser dado livremente (de forma implícita, não viciada: deve depender exclusivamente da vontade da pessoa, como em qualquer crime cujo objeto genérico de proteção seja a liberdade em qualquer das suas expressões).

A reforma motivada pela aprovação da LO 10/2022 também ajustou as penas associadas aos crimes sexuais. Por exemplo, a agressão sexual sem penetração era anteriormente punida com 1 a 5 anos de prisão, enquanto a nova lei estabelece um intervalo de 1 a 4 anos. No caso das agressões com penetração, a pena mínima é reduzida de 6 para 4 anos, enquanto a pena máxima se mantém nos 12 anos. Estas alterações têm sido objeto de controvérsia, especialmente devido ao efeito da sua aplicação retroactiva em benefício dos delinquentes condenados. A aplicação retroactiva da lei, princípio básico do direito penal quando uma norma favorece o delincente, levou à revisão de numerosas sentenças definitivas. Este efeito imprevisto gerou um intenso debate sobre a necessidade de ajustar a lei para evitar consequências indesejadas, o que foi finalmente feito pela LO 4/2023, de 27 de abril.

Não há dúvida de que a Lei Orgânica n.º 10/2022 foi orientada por um objetivo louvável de proteção da liberdade sexual, unificando os crimes e privilegiando o consentimento. No entanto, a redução das penas em certos casos evidenciou a complexidade da reforma do CP, pelo que é essencial que futuras alterações considerem detalhadamente as implicações práticas das alterações legislativas para garantir a proteção efectiva das vítimas e a punição adequada dos autores. A controvérsia acima descrita decorre do facto de se ter tocado nos limites máximos e mínimos penais sem prever a possibilidade de introduzir uma disposição transitória. O CP, em democracia, é um instrumento extremamente importante e deve manter-se à margem de ideologias e sectarismos.

2. HIPÓTESE

É verdade que a legislação a aplicar é a mesma em Madrid e em Barcelona, e que as condições para a sua aplicação são idênticas, o que significa que a abordagem jurídica inicial - e as suas vicissitudes - serão basicamente as mesmas. No entanto, se atentarmos no modelo TAS acima descrito, torna-se claro que, aceitando que o contexto em que o potencial delincente desenvolve as suas actividades modificará o seu comportamento, está implícito que as estratégias e recursos que podem ser perfeitamente úteis na província de Madrid não têm necessariamente o mesmo valor de aplicabilidade noutro ecossistema criminoso-delinquente diferente, como o da província de Barcelona, no qual, além do mais, funciona sob o controlo de forças policiais e modelos penitenciários também diferenciados.

Consequentemente, o interesse deste artigo assenta na formulação e estudo de uma hipótese básica: as agressões sexuais perpetradas na província de Madrid devem ser, de alguma forma e na medida em que são mediadas por diferentes modelos de ação situacional, significativamente diferentes das agressões sexuais cometidas na província de Barcelona.

3) METODOLOGIA

É verdade que a investigação criminológica não encontra dados suficientes ou adequados nas diferentes bases de dados públicas em Espanha para testar as suas abordagens. O problema, já amplamente criticado por outros investigadores, reside no facto de esta informação ser recolhida para fins público-administrativos que respondem às competências do órgão competente e, por isso, raramente tem em conta as necessidades dos investigadores e tende a satisfazer outros critérios que não são coerentes com as pretensões da ciência (Linde e Aebi, 2021). Particularmente excepcional é, no entanto, a informação disponibilizada pelo Centro de Documentação Judiciária (CENDOJ) do Conselho Geral da Magistratura (CGPJ), que oferece dados não filtrados, permitindo aos investigadores o seu tratamento de acordo com as suas necessidades específicas. No entanto, tendo em conta outras lacunas inerentes à própria natureza desta base de dados, a documentação que disponibiliza deve ser devidamente categorizada e filtrada, com base em critérios de partida muito específicos (Janosch, Pérez-Fernández, Nut e Marset, 2023). Por último, mas não menos importante, as informações fornecidas pelo CENDOJ são anónimas, públicas e isentas de direitos de autor.

Tendo em conta o exposto, foram analisados para este estudo 76 casos de agressões sexuais cometidas por um agressor inicialmente desconhecido da vítima nas províncias de Madrid e Barcelona, com base na análise de decisões judiciais publicadas na base de dados CENDOJ. A dimensão da amostra corresponde a uma representação do número total de agressões sexuais conhecidas e julgadas cometidas por agressores desconhecidos nas províncias indicadas. Os critérios de inclusão delineados foram os seguintes:

1. O agressor sexual era um homem desconhecido da vítima até pelo menos 24 horas antes do crime e actuava sempre sozinho.
2. A vítima, sempre do sexo feminino, tinha idade igual ou superior a 16 anos no momento da infração.
3. Os casos são legalmente definidos, na própria sentença, como "agressões sexuais" (penetração efectiva ou, pelo menos, tentativa de penetração com um pénis, através da vagina, boca e/ou ânus; ou penetração efectiva com dedos ou outros objectos, através da vagina e/ou ânus).

Com base nestes critérios de inclusão, foram encontrados, por acaso, 38 crimes na província de Madrid e 38 na província de Barcelona. As análises subsequentes foram efectuadas utilizando o pacote estatístico R versão 4.4.2 (2024), *Pile of Leaves*, Copyright (C) 2024 The R Foundation for Statistical Computing. Bibliotecas utilizadas: *vegan*, *ggplot2*, *ggrepel*, *cluster*, *factoextra*, *readxl*, *mclust* e *clue*.

3.1. CATEGORIZAÇÃO DOS ACÓRDÃOS

A fim de compilar corretamente os dados dos acórdãos para posterior análise estatística, foram seguidos os critérios e nomenclaturas descritos abaixo:

- Registo criminal do arguido. Estes são codificados em variáveis denominadas *Ag_Sex* (registo judicial por crime sexual), *Ag_Theft* (registo judicial por roubo), *Ag_Viol* (registo judicial por violência não sexual) e *Ag_Unesp* (registo judicial por crime não especificado). Estas variáveis foram codificadas na base de dados

da seguinte forma: 0 se o infrator não tiver antecedentes ou problemas psiquiátricos, 1 se tiver, e 2 se nenhum destes for referido na sentença.

- Variáveis situacionais específicas. Um grupo de sete variáveis responde a circunstâncias situacionais relacionadas com a própria violação - podem ser consideradas como "cenográficas". A vítima pode ou não ter resistido à prática do crime (*Ver_Resistir*); pode ou não ter gritado por socorro (*Ver_Gritar*); terceiros, como eventuais testemunhas ou forças policiais alertadas pelo acontecimento, podem ou não ter estado presentes durante a prática da violência sexual (*Ver_Terceiros*); ou a violação pode ou não ter sido interrompida por algum motivo (*Ver_Inte*). No que respeita ao agressor sexual, assume-se que este poderá ter actuado sob o efeito do álcool (*Ver_Alc*), ou de drogas (*Ver_Droga*), ou poderá mesmo ter tido as suas capacidades volitivas e intelectuais diminuídas (*Ver_Vic*). Em todos os casos detectados, as variáveis foram codificadas como 0 (ausência do comportamento), 1 (presença do comportamento) ou 2 (comportamento não referido na frase).
- Comportamento sexual do infrator. As variáveis seguintes assumem três valores possíveis, sendo que 0 indica ausência de conduta, 1 indica presença de conduta e 2 indica conduta não registada no processo judicial. As variáveis *Ver_Vag*, *Ver_Anal* e *Ver_Fel* indicam que a vítima sofreu penetração com o pénis na vagina, no ânus ou na boca, respetivamente. As variáveis *Ver_Vag_Tentativa* e *Ver_Anal_Tentativa* indicam que o agressor sexual tentou, sem sucesso, penetrar a vítima com o pénis na vagina ou no ânus, respetivamente. A variável *Ver_Finger* indica que o agressor penetrou a vítima com os dedos na vagina ou no ânus.
- Comportamentos não sexuais do agressor. Estas variáveis também assumiram os valores 0 (ausência), 1 (presença) e 2 (sem registo). Se o agressor se aproximou da vítima através de uma manobra enganosa, a variável *Ver_Con* foi codificada com 1. Se o agressor atacou a vítima de surpresa, então a variável *Ver_Surp* foi codificada com 1. Se utilizou algum tipo de arma (normalmente uma faca), a variável *Ver_Weap* foi codificada com 1. Se a vítima foi roubada de algum tipo de valor (dinheiro, telemóvel, cartão de crédito, etc.), a variável *Ver_Val* foi codificada com 1. Se o roubo foi de objectos pessoais (roupa interior, fotografias, agenda, etc.) que poderiam ser utilizados para algum fim fetichista, a variável *Ver_Pers* foi codificada com 1.
- Outras variáveis. Surgiram em relação a outras questões alternativas suscitadas pelos acórdãos e que têm interesse para a análise pormenorizada dos processos. Assim:
 - a. O agressor sexual demonstrou conhecimentos forenses nos seus comportamentos (utilização de preservativos, luvas, comportamentos de limpeza, etc.)? Em caso afirmativo, a variável *Ver_Fore* foi codificada com 1.
 - b. O agressor sexual actuou entre as 22:00 e as 6:00 horas locais? Em caso afirmativo, a variável *Ver_Darkness* foi codificada como 1.
 - c. O infrator agiu entre o meio-dia de uma sexta-feira e o meio-dia da segunda-feira seguinte? Se a resposta a esta pergunta foi afirmativa, a variável *Ver_Wend* (*fim de semana*) foi codificada como 1.

4. RESULTADOS

A Tabela 1 mostra a presença percentual das variáveis acima descritas nas sentenças por agressão sexual referentes às províncias de Madrid e Barcelona. Como se pode observar na Tabela 2, duas variáveis têm uma diferença significativa entre Madrid e Barcelona, e uma variável não é significativa, mas está no limite de significância $-p \leq 0,05$ -. Também se pode observar que os agressores sexuais actuam mais sob a influência de drogas e usam mais armas na província de Barcelona do que em Madrid. No entanto, são cometidas mais penetrações vaginais nos casos detectados em Madrid do que nos condenados em Barcelona.

Tabela 1. Percentagens de "presença" dos diferentes comportamentos referidos aos crimes analisados.

Variáveis	Significado	Madrid	Barcelona
Ag_Sex	Registo criminal do infrator por crimes sexuais.	5,3%	13,2%
Ag_Theft	Registo criminal do assaltante por roubo.	13,2%	13,2%
Ag_Viol	Registo criminal do infrator de violência não sexual.	10,5%	10,5%
Ag_Unesp	Registo judicial por crime não especificado.	15,8%	15,8%
Ver_Resist	A vítima resistiu.	52,6%	60,5%
Ver_Shout	A vítima gritou.	23,7%	28,9%
Ver_Terceiro	Apareceram terceiros alertados.	31,6%	18,4%
Ver_Inte	A agressão sexual foi interrompida por circunstâncias inesperadas.	28,9%	34,2%
Ver_Alc	O agressor estava sob o efeito do álcool.	5,3%	21,1%
Ver_Droga	O agressor estava sob o efeito de drogas.	5,3%	28,9%
Ver_Vic	O autor do crime tinha capacidades volitivas e intelectuais diminuídas.	7,9%	18,4%
Ver_Vag	A vítima sofreu penetração vaginal.	76,3%	50,0%
Ver_Anal	A vítima sofreu penetração anal.	7,9%	15,8%
Ver_Fel	A vítima sofreu penetração oral (fellatio).	34,2%	47,4%
Ver_Vag_Attempt	Houve uma tentativa mal sucedida de penetração vaginal.	7,9%	13,2%
Ver_Anal_Attempt	Houve uma tentativa mal sucedida de penetração anal.	10,5%	10,5%
Ver_Finger	O agressor penetrou a vítima com os dedos na vagina ou no ânus.	13,2%	13,2%
Ver_Con	O agressor abordou a vítima de forma enganosa.	55,3%	36,8%
Ver_Surp	O agressor aproximou-se da vítima de surpresa.	44,7%	63,2%
Ver_Weap	O agressor usou algum tipo de arma.	23,7%	47,4%
Ver_Vehi	O agressor dirigiu-se para o local do ataque num veículo.	10,5%	5,3%
Ver_Val	O agressor roubou activos financeiros da vítima.	36,8%	36,8%
Ver_Pers	O agressor levou um objeto que poderia ser utilizado como fetiche.	7,9%	5,3%
Ver_Fore	O agressor demonstrou conhecimentos forenses.	5,3%	15,8%
Ver_Darkness	A agressão foi cometida entre as 22:00 e as 6:00 horas.	42,1%	39,5%
Ver_Wend	O roubo foi cometido durante o fim de semana (entre o meio-dia de sexta-feira e o meio-dia de segunda-feira).	71,1%	60,5%

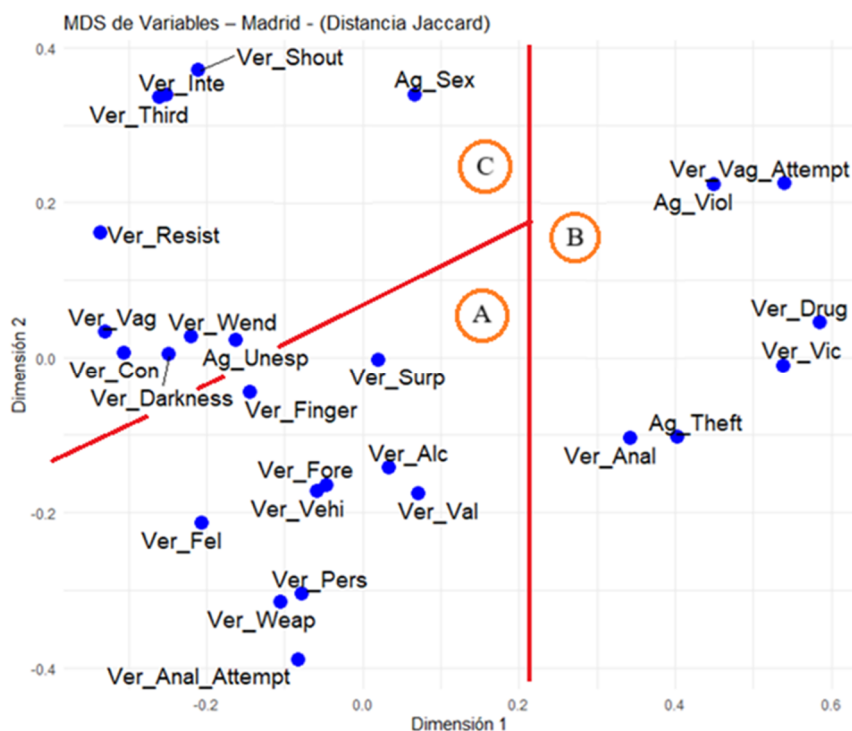
Tabela 2: Variáveis que revelaram diferenças significativas entre agressões sexuais cometidas por desconhecidos em Madrid e Barcelona.

Variável	valor de p	Teste utilizado
Ver_Droga	0,012	Exato de Fisher
Ver_Vag	0,032	Qui-quadrado
Ver_Weap	0,055	Qui-quadrado

O resultado do procedimento de escalonamento multidimensional (MDS) para os casos de Madrid pode ser visto na Figura 1. Os 3 clusters encontrados (A, B e C, na figura), formados pelos agrupamentos dos dados e que determinam outras tantas tipologias, foram encontrados através da análise *de agrupamento K-Means*. As tipologias detectadas na província de Madrid, analisadas de forma independente, seriam as seguintes

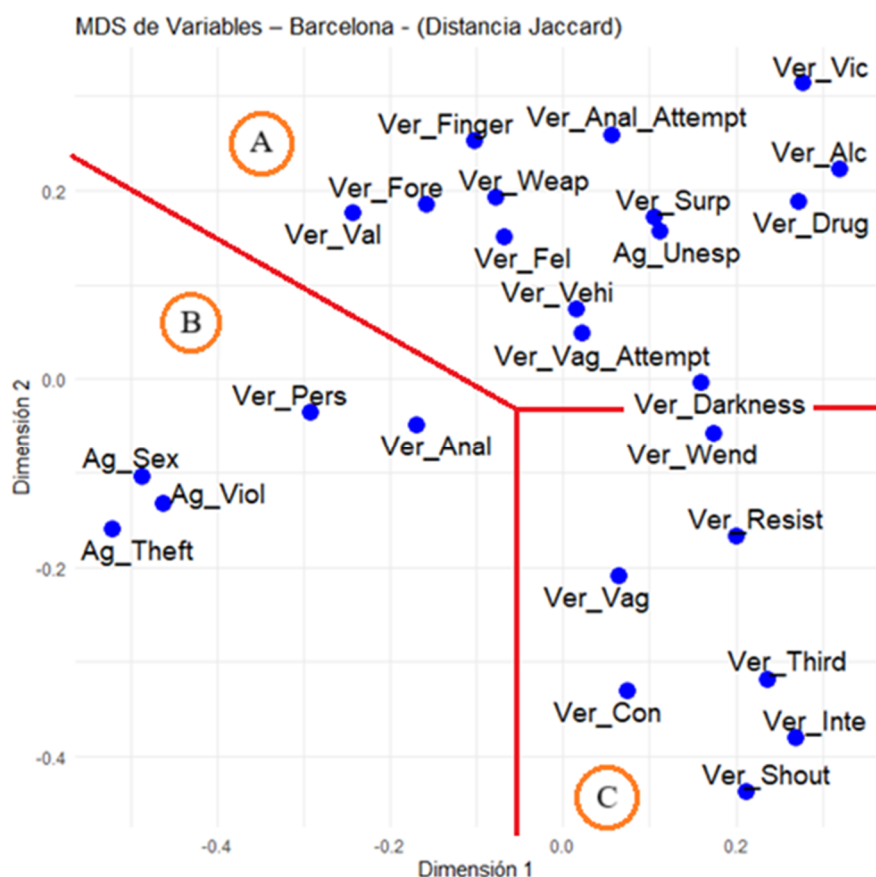
- O tipo A, impulsivo, é uma pessoa com antecedentes de outras agressões sexuais, que actua normalmente às escuras, durante o fim de semana, e aborda a vítima utilizando algum tipo de subterfúgio. No entanto, muitas vezes a vítima resiste e grita, alertando terceiros, pelo que a violação, apesar da existência de penetração anal ou vaginal, é interrompida. Ainda assim, a vítima pode ser roubada de objectos de valor.
- O tipo B, de natureza versátil, mostra um agressor sexual que actua sob a influência de drogas e, portanto, tem capacidades intelectuais e/ou volitivas diminuídas. Neste caso, em que o agressor pode ter antecedentes de roubo e de outros crimes violentos, há normalmente uma tentativa mal sucedida de penetração vaginal, bem como de penetração anal. Possivelmente, poder-se-ia pensar numa pessoa com um raciocínio deficiente, inicialmente motivada pelo roubo, que tenta tirar partido da ocasião.
- O tipo C sugere a presença de um agressor sexual planeador e mais especializado, com alguma consciência forense, que se desloca num veículo e que utiliza algum tipo de arma durante a agressão para intimidar e subjugar a vontade das suas vítimas. Neste caso, o agressor consome habitualmente álcool, obrigando a vítima a fazer felação, podendo tentar a inserção vaginal com os dedos e a penetração anal. Este terceiro tipo de agressor costuma retirar objectos da vítima para os utilizar como fetiches ou troféus.

Figura 1: Escala multidimensional das agressões sexuais cometidas em Madrid.



Tal como no caso anterior, os 3 clusters (A, B e C na figura), formados pelos agrupamentos dos dados, foram encontrados através da análise *de agrupamento K-Means*. As tipologias detectadas na província de Barcelona são as seguintes:

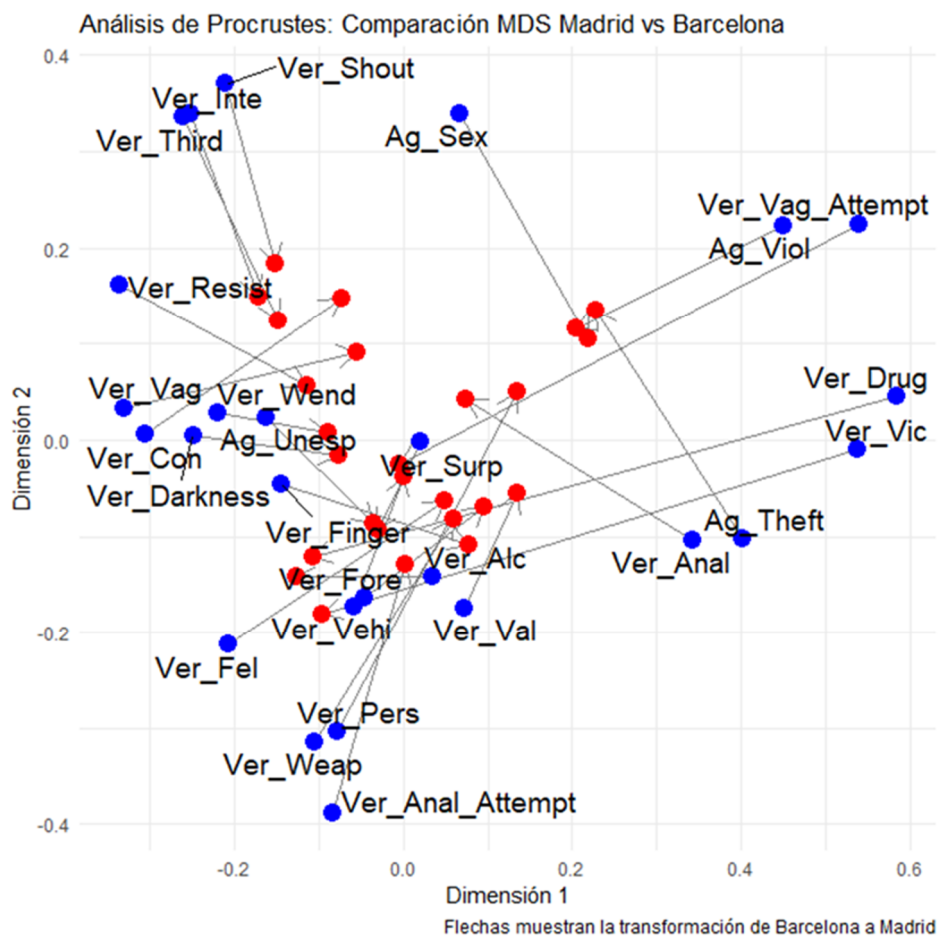
- O tipo A, parcialidade ocasional, seria uma pessoa com alguma consciência forense, que se desloca num veículo, consome drogas e tem antecedentes de outras infracções não especificadas na sentença. Esta pessoa, muitas vezes utilizando armas para dominar a vítima e sob o efeito de drogas e álcool, aborda as suas vítimas de surpresa e pode tentar obrigá-las a fazer-lhe sexo oral. Tenta, depois de introduzir os dedos nos órgãos genitais da vítima, e indistintamente, proceder à penetração anal e/ou vaginal, mas geralmente não consegue.
- O tipo B, muito versátil, policriminoso e, por conseguinte, pouco definido, é um delinquente com antecedentes de outros crimes sexuais, de roubo e de violência não sexual, que retira da vítima objectos sem valor aparente que podem ser utilizados como fetiches.
- O tipo C, de viés casual e recreativo, actua à noite e geralmente aos fins-de-semana. Aborda a vítima com artifícios e/ou subterfúgios diversos para proceder à penetração vaginal, mas na ausência de armas ou de um planeamento prévio que facilite as suas actividades, a vítima resiste, grita e alerta terceiros que possam interromper a agressão.

Figura 2: Escala multidimensional das agressões sexuais cometidas em Barcelona.

Para efetuar uma comparação entre as agressões e tipologias presentes em ambos os contextos, aplicou-se o teste de Procrustes aos escalões multidimensionais (MDS) que mostram os clusters/tipologias de Madrid e Barcelona, de forma a obter o melhor ajuste entre os dois. Após este processo, foram calculados o Índice de Jaccard (0,393) e o Índice ARI (0,332). O resultado foi uma sobreposição e diferenciação das tipologias descritas para cada um dos contextos de crime. A Figura 3 apresenta-se como o resultado do teste de Procrustes para comparar o resultado do MDS aplicado aos dados de Madrid com o resultado do MDS aplicado aos dados de Barcelona⁴. Neste ponto, é importante referir que a análise de Procrustes é útil para avaliar a semelhança entre duas configurações espaciais - ou nuvens - de dados. Os resultados obtidos por este procedimento mostram, portanto, como se alinham as configurações espaciais dos dados de Madrid e Barcelona após uma transformação óptima (rotação, escala e translação) destinada a minimizar ao máximo as diferenças entre elas.

⁴ A análise de Procrustes é um processo de transformação euclidiana dentro da série de métodos estatísticos que aplicam a teoria dos grupos à análise de conjuntos de dados homogêneos, a fim de os comparar entre si e fazer inferências a partir dessas comparações. É um dos procedimentos incluídos na chamada "análise estatística multivariada". O seu nome vem do mito de Procrustes, um dos filhos de Poseidon, que também era um terrível assassino em série. Tinha uma casa onde oferecia alojamento aos viajantes cansados que se aventuravam na zona. Aí convidava-os a deitarem-se numa cama de ferro que, enquanto dormiam, amarrava de pés e mãos aos seus quatro cantos. Se a vítima propiciatória fosse tão alta que o seu corpo fosse mais comprido do que a cama, Procusto cortava-lhe as partes salientes do corpo. Se fosse mais baixo que a cama, então ele martelava a vítima para a esticar até às dimensões corretas (Hurley e Cattell, 1962; Gower, 1975).

Figura 3: Comparação entre os IDS das províncias de Madrid e Barcelona.



4.1. TIPOLOGIAS A

No caso de Madrid, como já foi referido, este cluster agrupa variáveis relacionadas com crimes em que há roubo de objectos ou uma agressão menos violenta em termos físicos. Em Barcelona, no entanto, neste grupo predominam os agressores com antecedentes de crimes violentos e roubos, sem variáveis que indiquem diretamente violência sexual consumada.

As principais diferenças entre os dois ambientes têm a ver com os antecedentes criminais, uma vez que no caso de Barcelona há uma elevada presença de criminosos com antecedentes de crimes sexuais, roubo e violência. Em Madrid, pelo contrário, o grupo está mais relacionado com o roubo de bens materiais, troféus ou fetiches. Também se registam variações significativas no que se refere à agressão sexual propriamente dita. Enquanto nos casos da província de Barcelona se verifica uma maior relação com a penetração anal, em Madrid observam-se tentativas infrutíferas de penetração anal e agressão com os dedos ou felação.

Regra geral, pode indicar-se que no grupo A, em Madrid, há mais casos de engano, subterfúgio ou desculpa para abordar a vítima e de roubo, ao passo que em Barcelona os antecedentes criminais do infrator se tornam um fator-chave a ter em conta na avaliação da sua potencial perigosidade.

4.2. TIPOLOGIAS B

No que se refere a Madrid, as variáveis incluídas neste cluster apontam para um perfil de agressores com antecedentes judiciais por crimes violentos e/ou sexuais, bem como para circunstâncias em que o agressor se encontra sob o efeito de substâncias diversas. A vítima, por sua vez, sofre agressão sexual consumada ou tentada. No que diz respeito a Barcelona, as variáveis fornecem um perfil de agressores sem antecedentes criminais específicos, mas com características que reflectem um planeamento claro do ataque e um consumo de substâncias.

As principais diferenças em termos de registos criminais são que, para Madrid, há uma presença mais clara de registos por roubo e violência, enquanto em Barcelona há uma categoria bastante mais ambígua de registos não especificados. No que se refere ao modo de atuação do agressor, nos casos de Barcelona há mais indícios de planeamento, como o demonstra a presença muito sistemática do uso de artifícios, veículos e armas. Em Madrid, no entanto, a violência direta parece desempenhar um papel muito mais relevante.

No que diz respeito ao uso de substâncias e à agressão sexual propriamente dita, em ambos os casos observa-se a presença de drogas ou álcool, mas em Madrid a violência sexual é mais evidente em termos de agressão consumada. Em Barcelona, dentro do tipo B, há uma maior tendência para tentativas de agressão sem sucesso, mas com métodos mais diversos, como a penetração com os dedos.

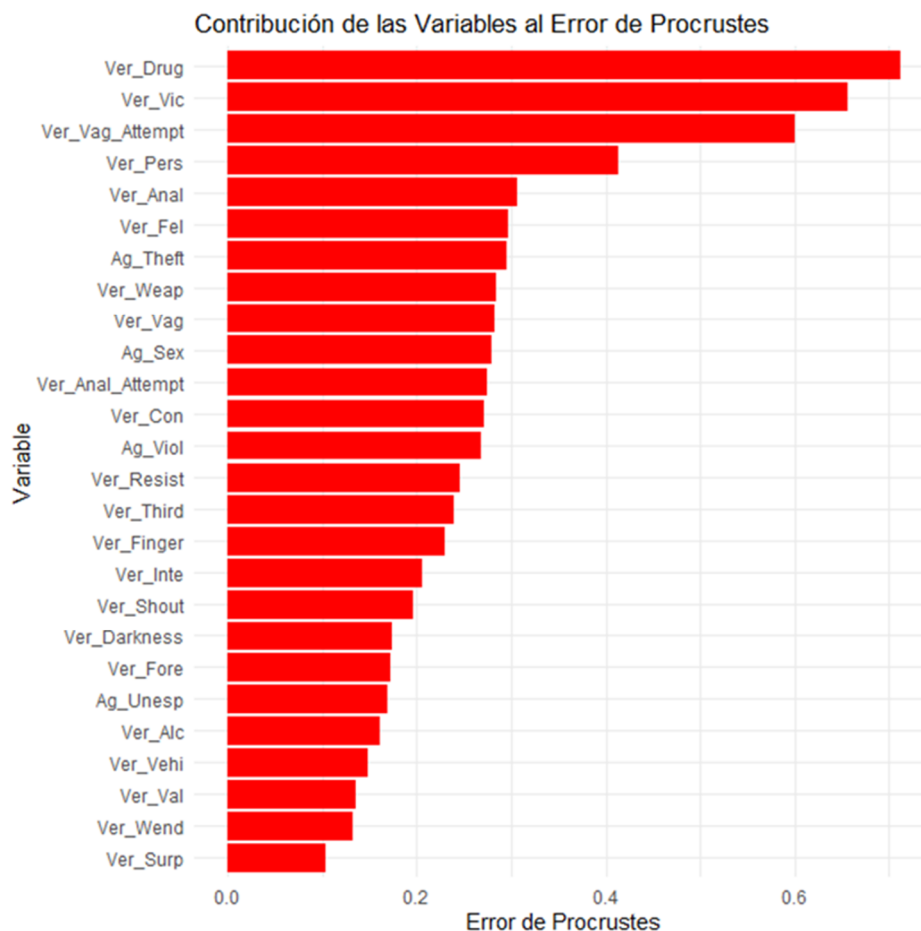
4.3. TIPOLOGIAS C

No contexto de Madrid, as variáveis deste cluster reflectem agressores que não têm necessariamente antecedentes judiciais graves, mas que actuam de forma impulsiva, sem grande planeamento e em ambientes em que a vítima tenta resistir e em que, normalmente, há intervenção de terceiros. No caso de Barcelona, também se verificam agressões interrompidas, mas com menor ênfase no uso de artifícios para abordar a vítima e com menor intervenção de terceiros que possam impedir o ataque.

As principais diferenças, no que diz respeito aos antecedentes criminais, prendem-se, em Madrid, com o facto de neste grupo se incluírem agressores com antecedentes de crimes sexuais, enquanto em Barcelona não há referência a esses antecedentes criminais. Como já foi referido, em ambos os casos há resistência por parte da vítima e uma eventual interrupção da agressão, mas em Madrid há mais variáveis associadas à presença de terceiros. De igual modo, nas agressões na província de Madrid, a ocorrência nocturna é um fator mais forte, enquanto que em Barcelona a variável do período noturno não aparece neste cluster.

A Figura 4, por outro lado, é ilustrativa, na medida em que representa a contribuição de cada variável para o erro de Procrustes - ou seja, para o desajuste dos dois conjuntos de dados. Isto indica quais os aspectos da agressão que mais diferem entre as configurações de dados encontradas entre os grupos de Madrid e Barcelona após a transformação.

Figura 4. Diferenças de cada uma das variáveis na posição espacial do MDS obtido com os dados de Madrid e os dados de Barcelona.



Ao analisar a interpretação geral dos resultados acima descritos, devem ser tidos em conta vários elementos:

1. Número de objectos e dimensões: 26 variáveis foram comparadas num espaço bidimensional.
2. Medida de ajuste (soma de quadrados de Procrustes): 2,6286, indica o nível de diferença entre as configurações antes e depois da transformação.
3. A raiz do erro quadrático médio de Procrustes (RMSE): 0,31796, representa a magnitude média do erro no alinhamento dos pontos (Tabela 3).

Distribuição dos erros quadráticos médios encontrados na análise de Procrustes.

Erro mínimo	0,1041
Primeiro quartil (Q1)	0,1719
Médio	0,2568
Terceiro quartil (Q3)	0,2919
Erro máximo	0,7121

Tendo em conta tudo o que precede, o que os dados da Tabela 3 sugerem é que a maioria das variáveis tem um erro de ajustamento relativamente baixo, mas há algumas

com erros mais elevados. De qualquer modo, para conseguir o melhor ajuste possível dos gráficos apresentados nas figuras 1 e 2, foi necessário efetuar uma rotação de 180°, com translação praticamente nula, e um escalamento de aproximadamente 0,5. Isto não implicou uma alteração significativa dos resultados e respondeu ao facto de o gráfico para a província de Barcelona ter uma dimensão linear de cerca de metade da obtida com os dados da província de Madrid, o que impedia a realização de comparações adequadas. O facto é que as configurações de Madrid e Barcelona são semelhantes em termos de estrutura, mas diferem em termos de escala e orientação. Este facto, por si só, indica que existem diferenças entre os dados das duas províncias que não podem ser ignoradas e que, portanto, estamos perante realidades diferentes em relação ao tema estudado. Assim, embora a correspondência entre os conjuntos de dados seja aceitável, alguns itens têm erros mais elevados que indicam diferenças na forma como certos tipos de agressão - e comportamentos do infrator - são estruturados em ambas as províncias.

Feita esta clarificação, uma observação mais atenta da Figura 3 mostra que os pontos azuis representam a configuração original de Madrid antes da transformação, enquanto os pontos vermelhos representam a configuração transformada de Barcelona para se alinhar com a de Madrid. As setas mostram a magnitude e a direção do ajustamento necessário para alinhar Barcelona com Madrid. Como se pode ver nos resultados numéricos, a estrutura de Barcelona foi rodada quase 180°, bem como redimensionada a partir do procedimento de Procrustes, de modo a alinhá-la com a de Madrid. Isto é evidente porque alguns dos pontos azuis e vermelhos estão em posições opostas em determinadas áreas. Os pontos com linhas mais longas relativos à mesma variável indicam que existem diferenças significativas na representação dessa variável entre as duas cidades. Por exemplo, *Ver_Droga*, *Ver_Vic* e *Ver_Vag_Tentativa* apresentam grandes deslocamentos, sugerindo que a representação espacial de Madrid no MDS é diferente da de Barcelona.

Por outro lado, nas áreas com maior concordância, ou seja, onde as variáveis onde os pontos vermelhos e azuis estão próximos, sugerem-se estruturas semelhantes em ambas as províncias. Por exemplo: *Ver_Finger*, *Ver_Fore* e *Ver_Alc* apresentam uma menor deslocação, indicando que os seus padrões são semelhantes nas duas cidades. A estrutura geral dos tipos de agressões e dos comportamentos que lhes estão associados é semelhante nas duas cidades, mas com diferenças interessantes de orientação e de escala. Como já vimos, algumas variáveis apresentam maior discrepância, como nos casos de *Ver_Droga*, *Ver_Vic* e *Ver_Vag_Tentativa*, indicando que estes factores são percebidos ou estruturados de forma diferente em cada província. Outras variáveis têm estruturas semelhantes, sugerindo padrões comuns de agressão e resposta em ambas as cidades que a criminologia deve explicar para aprofundar o seu campo de investigação e não simplesmente assumir.

Estas diferenças nas estruturas dos SDM correspondentes de Madrid e Barcelona devem necessariamente estar relacionadas com as tipologias encontradas pelo procedimento *K-Means*. Veja-se agora a Figura 4, que ajudará a clarificar numericamente o que se está a passar. As variáveis com maior erro de Procrustes - ou seja, as que mais diferem entre as duas cidades - são:

- *Ver_Droga* (0,71): O infrator estava sob a influência de drogas.
- *Ver_Vic* (0,66): As capacidades volitivas e intelectuais do infrator estavam diminuídas.

- *Ver_Vag_Attempt* (0,60): Houve uma tentativa de penetração vaginal sem êxito.
- *Ver_Pers* (0,41): O autor do crime roubou um objeto que poderia ser utilizado como fetiche.
- *Ver_Anal* (0,30): A vítima sofreu penetração anal.
- *Ver_Fel* (0,29): A vítima sofreu penetração oral (fellatio).
- *Ag_Theft* (0,29): Registo criminal do infrator por roubo.
- *Ver_Weapon* (0,28): O agressor usou algum tipo de arma. Há diferenças nas agressões em que o agressor usa uma arma, sendo mais frequente em Barcelona.
- *Ver_Vag* (0,28): A vítima sofreu penetração vaginal.

5. DISCUSSÃO

Parece claro que o estudo comparativo entre agressões sexuais cometidas por desconhecidos nas províncias de Madrid e Barcelona revelou diferenças significativas no modo como estes crimes são perpetrados em cada um dos contextos e que, por isso, a hipótese inicial é cumprida. Com base na análise de 76 casos extraídos de acórdãos judiciais e examinados através de testes estatísticos robustos - teste exato de Fisher, qui-quadrado, escalonamento multidimensional e análise de Procrustes - foram identificados padrões distintivos nas agressões sexuais cometidas em ambos os territórios.

Em termos de relevância da estatística utilizada, a utilização do teste exato de Fisher e do qui-quadrado para comparar a presença de determinadas características nos crimes cometidos em Madrid e Barcelona permitiu estabelecer diferenças significativas - ou quase significativas - em aspectos fundamentais como o consumo de drogas pelo agressor (*Ver_Drogas*, $p = 0,012$), o uso de armas (*Ver_Armas*, $p = 0,055$, no limite da significância) e a penetração vaginal (*Ver_Vag*, $p = 0,032$). Estes testes foram adequados para avaliar associações entre variáveis categóricas num conjunto de dados representativo mas relativamente pequeno.

As análises MDS e *K-means* permitiram-nos identificar tipologias de agressores e padrões de agressão em cada província, mostrando diferenças estruturais na forma como estes crimes são cometidos. A análise de Procrustes mostrou - sempre dentro da amostra de referência, o que deve levar a uma cautela razoável - que, embora haja uma estrutura semelhante de agressões sexuais em ambas as áreas, a escala e a orientação dos factores diferem significativamente, indicando padrões específicos em cada área.

No que diz respeito às diferenças entre Madrid e Barcelona, a análise estatística e espacial dos dados revelou que, embora os crimes sexuais cometidos por desconhecidos apresentem semelhanças estruturais em Madrid e Barcelona, existem diferenças importantes nos métodos e circunstâncias das agressões que apelam à importância de um estudo pormenorizado de ambos os ecossistemas criminais, tal como referido na introdução e previsto pelo TAS:

- Maior consumo de drogas pelos agressores em Barcelona: 28,9% dos agressores estavam sob a influência de drogas no momento da infração, em comparação com apenas 5,3% em Madrid. Isto pode indicar uma maior associação entre o consumo de substâncias e a agressão em Barcelona ou um contexto criminológico diferente, em que os infratores de Barcelona têm um maior historial de consumo de drogas no momento do ataque.

- Maior utilização de armas na província de Barcelona: 47,4% dos agressores utilizaram algum tipo de arma para dominar a vítima, enquanto em Madrid esta percentagem foi de 23,7%. Isto sugere um maior grau de violência instrumental nas agressões cometidas em Barcelona, o que pode estar relacionado com factores ambientais ou criminológicos específicos do contexto.
- Diferenças na forma de perpetrar a agressão sexual: em Madrid, a penetração vaginal foi mais frequente (76,3%) do que em Barcelona (50%). Mas, por outro lado, as agressões com penetração oral (fellatio) foram mais frequentes em Barcelona (47,4%) do que em Madrid (34,2%). Do mesmo modo, a penetração anal foi também mais frequente em Barcelona (15,8%) do que em Madrid (7,9%).
- Diferenças na estratégia de abordagem do agressor: em Madrid, os agressores utilizaram mais estratégias de engano, distração ou subterfúgio para abordar a vítima (55,3%) do que em Barcelona (36,8%). Em contrapartida, foi observado um maior número de ataques de surpresa e não planeados em Barcelona (63,2% contra 44,7% em Madrid). Isto sugere que os agressores da província de Barcelona optam mais frequentemente por ataques diretos e violentos, enquanto os de Madrid recorrem mais à manipulação e ao engano para reduzir a resistência da potencial vítima.
- Diferenças na reação da vítima e na interrupção do crime: as vítimas de Barcelona tenderam a resistir em maior proporção (60,5%) do que as de Madrid (52,6%). Talvez por isso, a interrupção da agressão por circunstâncias inesperadas foi mais frequente em Barcelona (34,2%) do que em Madrid (28,9%), o que sugere que em Barcelona as agressões tenderam a ocorrer em contextos menos controlados pelo agressor, facto que faz sentido dada a ideia de um maior uso da violência e, portanto, de uma componente de maior impulsividade e menor controlo prático da cena no agressor sexual desconhecido na província de Barcelona.
- Registos criminais do delinquente: os delinquentes em Barcelona tinham um maior número de registos de crimes sexuais anteriores (13,2%) em comparação com Madrid (5,3%). No entanto, não se registaram diferenças significativas nos registos de roubo ou de violência não sexual.

6. CONCLUSÕES

A partir dos resultados descritos neste estudo, é possível descrever um perfil de agressões sexuais por parte de estranhos encontrado nas sentenças emitidas em cada uma das províncias analisadas.

Em Madrid, verificou-se um maior recurso ao engano para abordar a vítima, uma maior frequência de penetração vaginal, um menor uso de armas e drogas no momento da agressão e um grupo de agressores com menos condenações anteriores por crimes sexuais. Em Barcelona, por outro lado, registou-se uma maior frequência de ataques de surpresa, um maior uso de armas e drogas e um maior número de agressores com antecedentes criminais por crimes sexuais. Foi também detectada uma maior frequência de agressões com penetração oral e anal, bem como uma maior tendência da vítima para resistir, embora com uma maior proporção de agressões interrompidas por factores externos.

Os resultados deste estudo confirmam que as agressões sexuais perpetradas por desconhecidos apresentam diferenças significativas nos dois territórios, sugerindo a necessidade de estratégias de prevenção e resposta adaptadas às especificidades

criminológicas de cada cidade. Isto, no contexto da TAS, só seria possível se se atentasse numa análise detalhada do contexto delinquente-criminal em que os agressores actuam em cada caso, o que exigiria estudos concretos, específicos, pormenorizados e detalhados que, muito simplesmente, põem em causa a validade da TAS, põem em causa a validade das grandes teorias e metodologias - que explicam o geral com certas garantias, mas tendem a falhar na abordagem do particular - e impõem a necessidade de um estudo cirúrgico de cada ecossistema criminal para a definição de políticas precisas e eficazes - de deteção, investigação e prevenção. Assim, por exemplo, este trabalho sugere que na província de Barcelona, dada a maior utilização de armas e drogas nos atentados, seria aconselhável implementar as medidas de controlo pertinentes sobre estes aspectos, bem como proceder a um estudo mais profuso, detalhado e rigoroso dos antecedentes criminais dos potenciais agressores. Em Madrid, no entanto, a acentuada tendência detectada para o recurso ao engano na abordagem à potencial vítima por parte do agressor sexual poderá indiciar a necessidade de campanhas de sensibilização que ajudem as mulheres a identificar o recurso a possíveis estratégias de manipulação, controlo e isolamento em estranhos.

Do ponto de vista criminológico, e tendo sempre em conta as variáveis ecossistémicas, os resultados evidenciam a importância de aprofundar a investigação sobre a relação entre os antecedentes criminais - a sua carreira criminal anterior, em geral - dos agressores e o seu comportamento durante a agressão, bem como as diferenças detectáveis na resposta específica das vítimas e os factores que podem levar à interrupção de um ataque, o que pode sugerir avanços e desenvolvimentos interessantes no quadro das políticas criminais a nível regional e mesmo provincial.

Por outro lado, é de salientar a relevância deste estudo para o desenvolvimento de técnicas criminológicas auxiliares da investigação policial e, mais concretamente, para o crescimento da caracterização criminológica indutiva - análise comportamental -, uma vez que os dados encontrados são úteis para a qualificação detalhada das actuais tipologias criminais que, muitas vezes, por serem excessivamente abrangentes, tendem a ser pouco úteis em termos da sua aplicação prática. Vemos, por exemplo, que na província de Madrid os agressores têm grupos mais diferenciados em função da gravidade do crime cometido, enquanto na província de Barcelona o agressor apresenta uma organização comportamental mais ligada à sua história criminal específica. Em ambos os casos, indistintamente, o consumo de substâncias e o planeamento do ataque desempenham um papel relevante, mas existem diferenças claras em termos de execução e interrupção do crime que devem ser conhecidas e devidamente matizadas, uma vez que seriam de grande ajuda para o desenho de perfis criminais específicos, bem como para os processos de investigação policial.

Em última análise, este estudo, que aqui apenas aborda duas províncias, mas que poderia ser alargado a nível nacional com financiamento e infra-estruturas adequados, contribui para uma melhor compreensão da violência sexual por parte de estranhos, ao mesmo tempo que mostra que um estudo situacional-ecológico do crime não só fornece dados úteis para melhorar a prevenção, a intervenção e a ação penal, mas também a sua compreensão criminológica para além das generalidades.

7. REFERÊNCIAS BIBLIOGRÁFICAS

- Arqué-Valle, P., Pastor-Cárcel, A., Roca-Mercadé, C. e Soria M.A. (2024). Influência cultural na motivação sexual de assassinos em série. *Logos Science & Technology Journal*, 16(1), 145-159, doi: <https://doi.org/10.22335/rlct.v16i1.1908>
- CGPJ (2023). Os tribunais concederam 1.205 reduções de pena em aplicação da Lei Orgânica 10/2022 [disponível em: <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/En-Portada/Los-tribunales-han-acordado-1-205-reducciones-de-pena-en-aplicacion-de-la-Ley-Organica-10-2022> , recolhido em março de 2024].
- Corovic, J., Christianson, S.A. e Bergman, R. (2012). Das acções na cena do crime na violação de estranhos à previsão do tipo de violador: vítima única ou violador em série? *Behavioral Science and the Law*, 30, 764-781.
- Domínguez Vela, M. (2016). Violência de género e vitimização secundária. *Revista Digital de Medicina Psicossomática e Psicoterapia*, Vol. 6(1). [disponível em: https://www.psicociencias.org/pdf_noticias/Violencia_de_geneo_y_victimizacion_secundaria.pdf , recuperado em maio de 2024].
- Gower, J.C. (1975). Análise generalizada de Procrustes. *Psychometrika*, 40, 33-51.
- Gutiérrez de Piñeres Botero, C., Coronel, E. e Pérez, C.A. (2009). Revisão teórica do conceito de vitimação secundária. *Liberabit* [online], 15(1), 49-58 [disponível em: https://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1729-48272009000100006 , recuperado em março de 2024].
- Hurley, J. R., e Cattell, R. B. (1962). The Procrustes Program: Producing direct rotation to test a hypothesized fator structure. *Behavioral Science*, 7(2), 258-262. <https://doi.org/10.1002/bs.3830070216>
- Janosch González, H. (2013). Fundamentos filosóficos da criminologia em Hirschi e Wikström: Popper ou Bunge? Em Serrano Maíllo, A., e Birkbeck, C., (Eds.) *A generalidade da teoria do autocontrolo. Uma primeira extensão da teoria geral do crime aos países de língua espanhola*. Madrid: Editorial Dykinson.
- Janosch, H., Pérez-Fernández, F., Nut, D. e Marset, M. (2023). Agressores sexuais desconhecidos da vítima em Espanha. Uma análise de escala multidimensional (MDE) baseada em uma análise de sentenças. *Revista de Derecho Penal y Criminología*, 3ª Época, 30, 395-411.
- Janosch, H., Pérez-Fernández, F. e Herrero, S. (2025). Agressores sexuais desconhecidos da vítima na Comunidade de Madrid: uma análise exploratória das sentenças proferidas pelo Tribunal Provincial. H. Janosch e F. Pérez-Fernández (coords.), *Panorámica de los delitos sexuales en España*. Madrid: Dykinson, 43-85.
- Janosch, H., Pérez-Fernández, F. e Popiuc, M. (2023). Baixo autocontrolo em homens não heterossexuais como um preditor de comportamentos de agressão sexual

- contra mulheres. *Behavior & Law Journal*, 9(1), 65-79, <https://doi.org/10.47442/blj.2023.100>
- Janosch, H., Pérez-Fernández, F., Popiuc, M. e López-Muñoz F. (2024). Relação entre baixa moralidade pessoal e sexo impessoal com comportamentos de agressão sexual contra mulheres numa amostra de homens heterossexuais espanhóis. *Journal of Asia Pacific Studies*, 7(2), 109-139.
- Janosch González, H., Pérez-Fernández, F. e Soto Castro, J.E. (2020). Um modelo de perfil para agressores sexuais desconhecidos que atacam em entradas de edifícios. *Revista de Derecho Penal y Criminología*, 3ª época, 24, 243-258.
- Kühne, H.H. (1986). *Kriminologie: Victimologie der Notzucht*. Juristische Schulung, 5, 388-394.
- Linde, A. e Aebi, M.F. (2021). Será que roubo significa realmente roubo? e outras equivalências duvidosas entre definições legais e criminológicas de infracções. Consequências para o estudo do crime. *Revista Española de Investigación Criminológica*, 19, Extra-2 [www.criminologia.net], <https://doi.org/10.46381/reic.v19i2.529>.
- Ministério do Interior de Espanha (2023). Anuário Estatístico do Ministério do Interior 2022. Catálogo de Publicações da Administração Geral do Estado: <https://cpage.mpr.gob.es>
- Pauwels, L., 2018a. Analisando o processo de percepção-escolha na Teoria da Ação Situacional. Um estudo de cenário aleatório. *Jornal Europeu de Criminologia*, 19(1), 130-147.
- Pauwels, L. (2018b). Os efeitos condicionais do autocontrolo na teoria da ação situacional. Um teste preliminar em um estudo de cenário randomizado. *Comportamento desviante*.
- Pérez-Fernández, F., Janosch, H. e Popiuc, M. (2023). Baixo autocontrole em homens não heterossexuais como um preditor de comportamentos de agressão sexual contra mulheres. *Behavior & Law Journal*, 9(1), 65-79. <https://doi.org/10.47442/blj.2023.100>
- Pueyo, A.A. e Redondo Illescas, S. (2007). Previsão da violência. Entre a perigosidade e a avaliação do risco de violência. *Papeles del Psicólogo*, 28(3), 157-173.
- Serrano Maíllo, A. (2017). *Crime, moralidade individual e controlos*. Valencia: Tirant Lo Blanch.
- Triviño, C., Winberg, M. e Moral, M. (2021). Credibilidade do testemunho em agressão e abuso sexual infantil: evolução do testemunho não crível na última década. *Behavior & Law Journal*, 7(1), 43-57. <https://doi.org/10.47442/blj.v7.i1.83>

- Wikström, P.-O., Oberwittler, D., Treiber, K. & Hardie, B. (2012). *Breaking Rules: The Social and Situational Dynamics of Young People's Urban Crime*. Oxford: Oxford University Press.
- Wikström, P.-O., & Treiber, K. (2016). Social Disadvantage and Crime: A Criminological Puzzle. *American Behavioral Scientist* 60(10), 1232-1259.



Artigo de investigação

DROGAS E CONDUÇÃO: METODOLOGIA DO RELATÓRIO SALIVAR SYNLAB "TOLERÂNCIA ZERO" E CRITÉRIOS DE APROVAÇÃO DO ORGANISMO NACIONAL DE ACREDITAÇÃO

Tradução para o português com ajuda de IA (DeepL)

Juan Carlos Rodríguez Bello

Cabo 1 da Guardia Civil

Agrupamento de tráfego da Guardia Civil

Perito universitário em criminalidade rodoviária pela UNED (UNED)

Perito judicial em matéria de controlo documental pela UNED (UNED)

jcrbello@guardiacivil.es

Recebido em 18/02/2025

Aceite em 14/05/2025

Publicado em 27/06/2025

Citação recomendada: Rodríguez, J. C. (2025). Drogas e condução: metodologia de "tolerância zero" do relatório salivar do laboratório Synlab e critérios de homologação da Entidade Nacional de Acreditação. *Revista Logos Guardia Civil*, 3(2), p.p. 197-220.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

DROGAS E CONDUÇÃO: METODOLOGIA DO RELATÓRIO SALIVAR SYNLAB "TOLERÂNCIA ZERO" E CRITÉRIOS DE APROVAÇÃO DO ORGANISMO NACIONAL DE ACREDITAÇÃO

Resumo: INTRODUÇÃO. 2. ESTRATÉGIA DA DIRECÇÃO-GERAL DE VIAÇÃO: "TOLERÂNCIA ZERO". 2.1. LÓGICA E PROCEDIMENTO PARA A REALIZAÇÃO DO TESTE SALIVAR DE DROGAS. 3. A DOUTRINA DA PROCURADORIA GERAL DO ESTADO APÓS O TESTE SALIVAR "POSITIVO" PARA DROGAS. 4. A PRESENÇA DE DROGAS NO ORGANISMO: A SANÇÃO ADMINISTRATIVA E A DOUTRINA DO TRIBUNAL CONSTITUCIONAL. 5. OS "PONTOS DE CORTE" E AS QUANTIDADES MÍNIMAS PSICOATIVAS. 6. A EMPRESA DE ANÁLISES CLÍNICAS SYNLAB. 7. OS LIMITES DE QUANTIFICAÇÃO E OS INTERVALOS DE INCERTEZA DO LABORATÓRIO SYNLAB. 8. O LABORATÓRIO SYNLAB E A SUA ACREDITAÇÃO PELO ORGANISMO NACIONAL DE ACREDITAÇÃO ATRAVÉS DE AUDITORIAS. 9. ÂMBITO DA ACREDITAÇÃO ENAC 1169/LE2347 CONCEDIDA AOS LABORATÓRIOS SYNLAB. 10. CONCLUSÕES. 11. REFERÊNCIAS BIBLIOGRÁFICAS. ANEXO I - COMPOSIÇÃO E PRINCÍPIOS DO DED (ANALISADOR) SOTOXA.

Resumo: A legislação relativa ao controlo do consumo de álcool e drogas tem um grande impacto na sociedade, nem sempre isento de controvérsia, dependendo da forma como essa informação é transmitida à opinião pública. Um exemplo claro são os critérios utilizados para estabelecer o limite legal de consumo de álcool compatível com a condução de veículos. Embora a sociedade aceite o critério de tolerância zero para o consumo de drogas, é essencial uniformizar os métodos utilizados para detetar e quantificar a presença de drogas que influenciam a condução e, consequentemente, afectam a segurança rodoviária. Neste contexto, o estabelecimento e a determinação da quantidade das concentrações mínimas, em caso de teste de despistagem positivo, são essenciais e especialmente importantes no caso de reincidentes ou de infractores rodoviários. No entanto, esta determinação qualitativa e quantitativa deve ser objeto de um controlo adequado. Este artigo passa em revista a história que conduziu à determinação das quantidades detectáveis de drogas, mas, sobretudo, os critérios de rastreabilidade típicos dos sistemas acreditados no domínio da segurança rodoviária.

Resumen: La legislación sobre el control del consumo de alcohol y drogas tiene una gran repercusión en la sociedad, no siempre exenta de polémica, dependiendo de cómo se traslade esta información a la opinión pública. Un claro ejemplo, lo tenemos con los criterios que se utilizan para establecer el límite legal de consumo de alcohol compatible con la conducción. Si bien es aceptado por la sociedad el criterio de tolerancia cero en cuanto al consumo de drogas, es fundamental la estandarización de los métodos por los que se detecta y cuantifica la presencia de drogas que influye en la conducción y, consecuentemente, afecta a la Seguridad Vial. En este contexto, establecer y determinar la cantidad de las concentraciones mínimas, en caso de detectarse un positivo en drogas, es imprescindible y especialmente importante en conductores reincidentes o en los delincuentes viales. Sin embargo, esta determinación cualitativa y cuantitativa debe estar debidamente auditada. En este artículo, se hace una revisión del histórico que ha llevado a la determinación de las cantidades detectables de drogas, pero, sobre todo, a los criterios de trazabilidad que son propios de sistemas acreditados en el ámbito de la Seguridad Vial.

Palavras-chave: Segurança rodoviária, tolerância zero, condução, drogas, detecção, concentração mínima, normalização, acreditação.

Palabras clave: Seguridad Vial, tolerancia cero, conducción, drogas, detección, concentración mínima, estandarización, acreditación.

ABREVIATURAS

Art.: Artigo.

PC: Código Penal.

DED: Dispositivo eletrónico de deteção (droga portátil).

DGT: Direção-Geral do Tráfico.

ENAC: Entidad Nacional de Acreditación (Entidade Nacional de Acreditação)

FSCSV: Procurador da Câmara de Coordenação da Segurança Rodoviária

FGE: Fiscalía General del Estado.

ISO: International Standardization Organization (norma reconhecida internacionalmente).

LOQ: Limite de quantificação.

LSV: Lei da segurança rodoviária.

Ng: Nanograma ($1\text{ng} = 1,0\text{E}-9\text{ g}$).

SV: Segurança rodoviária.

OMS: Organização Mundial de Saúde.

ONSV: Observatório Nacional de Segurança Rodoviária.

ONU: Nações Unidas.

SV: Segurança rodoviária.

TC: Tribunal Constitucional.

UNE: Uma norma espanhola.

UE: União Europeia.

1. INTRODUÇÃO.

No "Plano Global - Década de Ação para a Segurança Rodoviária¹ 2021-2030" da Organização Mundial de Saúde (OMS-ONU), foi determinado que um dos principais comportamentos que contribuem para as mortes e vítimas de acidentes rodoviários é a condução sob o efeito do álcool. Por conseguinte, a OMS insta os governos a: conceber o funcionamento de um sistema de transporte rodoviário seguro através da criação de leis de Segurança Rodoviária (SR), fazer cumprir essas leis e promover a educação para a segurança rodoviária. Além disso, o organismo da ONU insta não só os organismos oficiais, mas também as empresas privadas a abordarem e atenuarem as acções que afectam negativamente a segurança rodoviária e a divulgarem a mensagem de que o consumo elevado de álcool e de outras substâncias, como as drogas, contribui para uma "condução perigosa". A OMS estabelece igualmente dois objectivos para 2030: reduzir para metade o número de mortos e feridos em acidentes rodoviários provocados por condutores sob o efeito do álcool e conseguir uma redução dos acidentes provocados pelo consumo de substâncias psicoactivas.

Em relação ao exposto, em Espanha, o Observatório Nacional de Segurança Rodoviária (ONSV)² como organismo dependente do Ministério do Interior e gerido através da Direção-Geral de Viação (DGT), publicou a chamada "Revisão sistemática sobre drogas e condução (2021)". Este documento faz referência à "Lei de Trânsito, Circulação de Veículos Motorizados e Segurança Rodoviária" (LSV)³, e especificamente ao Art. 14, que proíbe a condução com a presença⁴ de drogas no corpo (excluindo as substâncias utilizadas sob prescrição médica e para fins terapêuticos). No entanto, nesta secção da LSV, o legislador alerta que "(...) desde que (o condutor) esteja apto a utilizar o veículo de acordo com a obrigação de diligência, prudência e não distração⁵ estabelecida no art.º 10.

Além disso, em Espanha, a condução de um veículo a motor "sob a influência de drogas tóxicas, estupefacientes ou substâncias psicotrópicas" pode constituir uma infração contra o SV, tal como definido no artigo 379.2 da Lei Orgânica 10/2015 do Código Penal (CP). Por este motivo, no dia 17 de julho de 2019, a Procuradoria Geral do Estado (FGE), através da Procuradoria para a Coordenação da Segurança Rodoviária (FSCSV), emitiu uma Instrução para a elaboração de atestados para os crimes de condução sob influência de tóxicos, estupefacientes e substâncias psicotrópicas do art. 379.º, n.º 2, do Código Penal. Nesta Instrução, destaca-se a importância do relatório de sinais exteriores para determinar a influência destas substâncias, uma vez que o legislador espanhol não dispunha de uma taxa objetiva para determinar a diminuição das faculdades

¹ Ver: <https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030>.

² Ver: <https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/subsecretaria-del-interior/direccion-general-de-traffic/>

³ Real Decreto Legislativo 6/2015, de 30 de outubro, que aprova o texto revisto da Lei de Trânsito, Circulação de Veículos Motorizados e Segurança Rodoviária do Interior. BOE n.º 261, de 31 de outubro de 2015 Referência: BOE-A-2015-11722.

⁴ Positivo para drogas: será aplicada uma coima por infração ao art. 14.1. 5ª da LSV para a presença de drogas (1000 Euros / 6 pontos)".

⁵ O condutor deve utilizar o veículo com a diligência, a prudência e o cuidado necessários para evitar qualquer dano, quer a si próprio quer a terceiros, tendo o cuidado de não o pôr em perigo a si próprio, aos outros ocupantes do veículo e aos outros utentes da estrada, especialmente aqueles cujas características os tornam mais vulneráveis".

psicofísicas do sujeito para uma condução segura e, portanto, o elemento típico da influência. Nas suas próprias palavras, "as teses aplicadas ao álcool não são transferíveis per se para as drogas tóxicas, estupefacientes e substâncias psicotrópicas, em que as premissas científicas diferem do álcool por várias razões", e isso deve-se ao facto de não ter sido possível estabelecer a influência sobre as aptidões psicofísicas do sujeito que lhe permitem conduzir com segurança, com base num nível de concentração de droga detectado num teste de saliva.

Assim, no nosso país e de acordo com os dados fornecidos pela DGT⁶, "quase um terço dos mortos em acidentes rodoviários excedeu o limite de álcool", mas também podemos afirmar, a partir da evidência da observação feita durante mais de duas décadas de prática profissional "na estrada" pelo autor deste trabalho de investigação, que o estilo de vida de lazer e de vida nocturna é um dos factores que aumentam a probabilidade de consumo de álcool e de drogas (cannabis, cocaína e ecstasy) por parte de alguns condutores (Calafat, A. et al, 2000). E este consumo tem vindo a consolidar-se cada vez mais nos últimos anos, tornando-se um dos factores de risco mais importantes para os acidentes rodoviários em Espanha.

Podemos também afirmar, graças à experiência profissional do autor, que outro fator de risco é a condução como passageiro de um veículo motorizado cujo condutor tenha consumido álcool ou drogas, o que provoca todos os anos um fluxo constante daquilo a que podemos chamar "vítimas inocentes" (passageiros, motociclistas, peões e ciclistas) que morrem em acidentes rodoviários em consequência da condução de um condutor sob o efeito do álcool ou de drogas, ainda que após a participação conjunta de ambos (condutor e passageiro) em actividades nocturnas associadas ao lazer.

É por isso que, apesar das políticas de VS da DGT, das suas campanhas de sensibilização para o consumo de álcool e de drogas antes da condução, das campanhas de vigilância e de controlo levadas a cabo pelos agentes de fiscalização do trânsito, não existe ainda uma verdadeira "sensibilização comunitária para a VS" ou uma "sensibilização social rodoviária" que nos faça compreender os perigos deste tipo de comportamento, mas sobretudo preveni-lo e, em todo o caso, enquanto condutores ou utentes, rejeitá-lo e denunciá-lo.

Por último, não podemos deixar de mencionar os condutores que são reincidentes ou múltiplos (classificados como tal de acordo com o tempo decorrido entre a prática de uma infração e outra e o número de infracções cometidas) e que, sendo consumidores habituais de álcool ou de drogas (ou de ambas as substâncias ao mesmo tempo), podem ser designados por "condutores toxicodependentes", podendo ser considerados potencialmente perigosos para a VS e devendo, por isso, ser sujeitos a um acompanhamento e tratamento especiais como doentes pelas autoridades sanitárias⁷, em coordenação com o trabalho de vigilância e controlo da DGT.

⁶Ver: https://revista.dgt.es/es/noticias/nacional/2022/04ABRIL/0404_Campana-alcohol-Cifal.shtml.

⁷O regulamento nacional RD 818/2009, Regulamento Geral para os Condutores, e os regulamentos europeus CD 439/1991, CD 126/2006 e CD 36/2012, estabelecem que estes doentes (toxicodependentes) não podem obter ou renovar a carta de condução por não terem aptidões adequadas para uma condução segura.

2. A ESTRATÉGIA DA DIRECÇÃO-GERAL DO TRÁFEGO: "TOLERÂNCIA ZERO".

Em junho de 2012, a DGT adoptou a medida de "tolerância zero" como a sua principal linha de estratégia em matéria de condução e consumo de drogas, aplicando esta "tolerância zero" a todos os condutores que consomem drogas e que se sentam ao volante de um veículo. As razões apresentadas pela DGT⁸ foram as seguintes: "A Espanha está entre os países com maior consumo de drogas, especialmente cocaína e canábis, o que resulta num aumento do risco de acidentes rodoviários e de lesões fatais ou graves".

Assim, de acordo com o estudo de 2017 do Observatório Europeu da Droga e da Toxicodependência (OEDT⁹), na faixa etária dos 15 aos 34 anos, a Espanha é a mais afetada pela toxicodependência na União Europeia:

É o sexto país da UE com a taxa mais elevada de consumo de cocaína (com uma prevalência de 2,8%), depois do Reino Unido (4,7%), dos Países Baixos (4,5%), da Dinamarca (3,9%), da França (3,2%) e da Irlanda (2,9%).

O quarto país da UE com a taxa mais elevada de consumo de cannabis (18,3%), atrás da França (21,8%), da Itália (20,9%) e da República Checa (19,3%).

Por conseguinte, as acções a empreender pela DGT, em conformidade com a sua estratégia de "tolerância zero", incluíam o seguinte

Sensibilizar a sociedade em geral para o problema, informar os condutores sobre o risco do consumo de drogas (sem esquecer o risco que representa o consumo de álcool), conhecer os consumos mínimos de álcool e de drogas que provocam uma diminuição importante da capacidade de condução, alargar os controlos de drogas e de álcool + drogas a todos os tipos de estradas, dias e horários; colaborar com outras administrações em matéria legislativa, educativa e de formação relacionada com a droga e a condução e promover a investigação aplicada no domínio da droga e da segurança rodoviária.

De igual modo, e como objetivo para o ano de 2030, a área estratégica de vigilância e controlo da DGT estendeu a "tolerância zero" aos comportamentos de risco com maior impacto na sinistralidade rodoviária, com as seguintes prioridades: atuar sobre o excesso de velocidade, o consumo de álcool e drogas, a utilização de telemóveis durante a condução e a não utilização de equipamentos de segurança (cintos de segurança, capacetes, sistemas de retenção para crianças, etc.).

2.1. FUNDAMENTOS E PROCEDIMENTOS DA ANÁLISE SALIVAR DE DROGAS.

Até há relativamente pouco tempo, e devido à inexistência de Dispositivos Electrónicos de Detecção (DED) portáteis com a tecnologia adequada, não era comum a realização de testes "na estrada" para detetar se o condutor tinha consumido drogas. A razão para tal é

⁸Documento "Drogas e Condução - Tolerância Zero" (DGT).

<https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2012/Presentacion-Tolerancia-cero-con-los-conductores-que-consuman-drogas-al-volante.pdf>

⁹Ver: https://www.euda.europa.eu/publications_en

que só através de uma análise ao sangue se podia ter a certeza dos resultados, mas, além disso, a realização destas análises ao sangue e a sua posterior transferência para o laboratório para análise era relativamente complexa e juridicamente difícil.

Posteriormente, a importância da questão e o empenho da DGT em detetar o consumo recente de drogas e a presença de drogas no organismo do condutor tornaram-se muito relevantes tanto para a SV como para o ambiente de trabalho do condutor profissional. Gradualmente, os testes de despistagem de drogas foram implementados com dispositivos portáteis DED¹⁰ que permitem a deteção e análise do consumo recente de drogas na saliva do condutor. Através da recolha rápida de amostras de fluido oral (como procedimento não invasivo), é possível obter um "indicativo positivo"¹¹ para o consumo recente de cinco drogas (anfetaminas, metanfetaminas, opiáceos, canábis e cocaína). No entanto, é necessário recolher uma segunda amostra de saliva, designada "teste probatório", para nomear e quantificar o tipo de droga detectado nesta segunda amostra e, assim, confirmar o "positivo indicativo" obtido; esta segunda análise da saliva será efectuada num laboratório de referência. A transferência para o laboratório deste "teste probatório" é efectuada num "tubo de recolha de saliva" selado e identificado com um código de barras, que é colocado numa geleira, depois de registado num documento regido por um protocolo rigoroso de cadeia de custódia.

A obrigatoriedade deste teste laboratorial complementar (teste probatório) após o controlo inicial (teste circunstancial) e a ratificação no laboratório de referência do tipo de droga detectada e da sua quantidade, dará presunção de veracidade legal à infração pela presença de drogas no organismo do condutor, bem como a correspondente abertura de um processo administrativo sancionatório pela DGT.

3. A DOUTRINA DA PROCURADORIA-GERAL DO ESTADO NA SEQUÊNCIA DO TESTE DE DESPISTAGEM DE DROGAS SALIVARES "POSITIVO".

De acordo com a doutrina da Procuradoria-Geral da República (FGE)¹², e uma vez obtido um "resultado positivo"¹³ no teste do índice salivar efectuado num DED portátil capaz de analisar fluidos orais, é obrigatória a análise subsequente da saliva num "laboratório aprovado", em função das actividades de controlo necessárias por parte da administração competente, garantindo também a "cadeia de custódia"¹⁴ da saliva recolhida para análise, a fim de assegurar a legalidade do procedimento de obtenção das amostras de saliva e a sua posterior conversão em provas de acusação. A FGE especifica ainda que os agentes encarregados da fiscalização do trânsito devem receber formação específica para o seu desempenho, uma vez que este tipo de teste é mais complexo do que os testes de deteção de álcool.

¹⁰ Ver: <https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html>

¹¹ Trata-se de uma amostra "indicativa" que detecta a eventual **presença** de substâncias ilícitas. Ver: <https://revista.dgt.es/es/sabia-que/normas/2018/0703como-se-hace-un-control-de-drogas.shtml>

¹² Circular 10/2011 de 17 de novembro (BOE FIS-C-2001-000010).

¹³ O termo "positivo" não indica uma determinada taxa em nanogramas, mas qualquer resultado que indique a mera presença de drogas no organismo, ou seja, não se trata de um teste quantitativo, mas de um teste de qualificação com um resultado positivo ou negativo.

¹⁴ A cadeia de custódia é entendida como o processo através do qual se acredita que o objeto apreendido é o mesmo que foi finalmente analisado. Uma eventual violação da cadeia de custódia pode conduzir a uma violação do direito a um processo equitativo.

Uma vez no laboratório, as amostras salivares são processadas por um equipamento analítico constituído por um cromatógrafo de gás¹⁵ (capaz de vaporizar substâncias de diferentes volatilidades) e um espectrómetro de massa¹⁶ (capaz de gerar iões a partir de moléculas neutras na fase gasosa, separando-os de acordo com a sua massa e detectando-os através do registo adequado da informação), determinando o tipo e a quantidade de droga presente na amostra salivar. Estes kits são capazes de detetar até quarenta tipos de drogas e quantidades tão pequenas como um nanograma¹⁷ (ng). Estes resultados laboratoriais são depois analisados um a um por pessoal médico especializado, que assina e valida o relatório final a enviar à DGT.

No entanto, como já indicámos, ao contrário dos testes de álcool, foi adoptada uma política de "tolerância zero" das SV no caso das drogas tóxicas, uma vez que o LSV¹⁸ proíbe expressa e tacitamente a presença de substâncias estupefacientes no corpo do condutor. Uma política rodoviária que não está isenta de críticas, uma vez que vários autores censuram a discrepância entre os resultados positivos detectados no DED e os resultados laboratoriais positivos (Ramírez, J, 2024).

Estes autores afirmam que os "cutoff" (pontos de corte analíticos determinados em ng/ml)¹⁹, das marcas de DED portáteis, os limites de detecção confirmados pelo laboratório e a quantidade de substância psicoactiva detectada não podem ser contrastados.

4. PRESENÇA DE DROGAS NO ORGANISMO: A SANÇÃO ADMINISTRATIVA E A DOCTRINA DO TRIBUNAL CONSTITUCIONAL.

A LSV impõe uma sanção administrativa de 6 pontos e uma coima de 1000 euros a quem conduzir com a presença de drogas no organismo. Neste ponto, mencionaremos o Plenário 174/2017 do Tribunal Constitucional²⁰ (TC), devido à questão de inconstitucionalidade levantada em relação a vários artigos do RD 339/1990²¹, e especificamente sobre a relevância de levantar uma questão de inconstitucionalidade em relação ao art. 12 da Lei 6/2015, ao classificar como uma infração administrativa a condução de um veículo "com a presença de drogas no seu corpo", sem que seja necessário provar que a presença dessas drogas influenciou a sua capacidade de conduzir. O Tribunal Superior "não considera que os preceitos impugnados sejam inconstitucionais por proibirem o consumo de drogas, através de uma norma que visa a proteção da VS". Esclarece ainda que os preceitos impugnados "não se destinam a proibir o consumo de drogas em geral". Portanto, o que proíbe é: condutores que conduzam "com a presença

¹⁵Ver:https://www.mncn.csic.es/docs/repositorio/es_ES/investigacion/cromatografia/espectrometria_de_masas.pdf

¹⁶ Universidade de La Rioja. Serviço de Laboratórios e Workshops. Cromatografia gasosa: Análise qualitativa por cromatografia gasosa de detecção em massa Sem operações prévias de preparação de amostras. 75 € / hora. Espectrometria de massa: Análise qualitativa por espectrometria de massa electrospray/alta resolução Sem operações prévias de preparação de amostras. 120 € / hora.

¹⁷ Milionésima parte de um grama: 1 ng = 1e-9 gr.

¹⁸ RD 6/2015 de 30 de outubro, alterado pela Lei 18/2022 de 20 de dezembro BOE n.º 304. Um ponto de corte é a concentração de uma substância a partir da qual um teste de diagnóstico é considerado positivo.

¹⁹ Um ponto de corte é a concentração de uma substância a partir da qual um teste de diagnóstico é considerado positivo.

²⁰ BOE n.º 15 de 17 de janeiro de 2018. Sec. TC.

²¹ BOE n.º 63, de 14 de março de 1990, que aprova o articulado da Lei de Trânsito, Circulação de Veículos Motorizados e Segurança Rodoviária.

de drogas no organismo (...)"'. Assim, é "tipificado como contraordenação, pelo que a conduta proibida que constitui contraordenação não é o consumo de drogas, mas sim a condução se este tipo de substâncias tiver sido consumido". Mas o que é ainda mais interessante é o facto de o Supremo Tribunal equiparar o consumo de tóxicos ao consumo de drogas sob prescrição médica e para fins terapêuticos, uma vez que: "O risco que a condução com a presença deste tipo de substâncias no organismo pode acarretar para a segurança do trânsito será o mesmo tanto no caso de as drogas consumidas estarem sob indicação médica como nos casos em que o consumo destas não seja para fins terapêuticos".

Em consequência, o TC não considera que os preceitos impugnados violem artigos constitucionais e que isso invalide a abordagem e o conceito do que se deve entender por "drogas"; aliás, garante que este conceito é definido como uma substância que tem entidade suficiente para alterar as capacidades psicofísicas de quem a consome, e que "O objetivo da norma, ao tipificar como contraordenação a condução com a presença de drogas no organismo, é o de impedir a condução de pessoas que tenham ingerido substâncias susceptíveis de alterar as condições psicofísicas para a condução, dado o risco que a condução nessas condições pode acarretar para a segurança do trânsito (...)"'.)

5. PONTOS DE CORTE E QUANTIDADES PSICOACTIVAS MÍNIMAS.

Mais uma vez, a DGT adverte, no documento "Revisão sistemática sobre drogas na condução" (2021), que não existem acordos internacionais ou nacionais sobre os pontos de corte (quantificados em ng/ml)²² a estabelecer nos procedimentos de controlo do consumo de substâncias nos condutores e que a Espanha foi um dos primeiros países a regulamentar o teste através de uma amostra de saliva. Para o efeito, a DGT afirma ter tido em conta os valores recomendados a nível internacional no domínio da segurança no trabalho, onde vários organismos de prestígio, como a Substance Abuse and Mental Health Services Administration (SAMHSA)²³ nos Estados Unidos, a European Workplace Drug Testing Society (EWDTS)²⁴, ou a National Safety Council's Alcohol, Drugs and Impairment Division (NSC-ADID)²⁵ na Europa e no Reino Unido), emitiram relatórios actualizados sobre as recomendações dos pontos de corte a estabelecer, em conformidade com os requisitos das normas ISO²⁶ /IEC²⁷ na Europa.

Assim, com base no exposto, o Ministério do Interior estabeleceu valores de positividade para a análise probatória em laboratório publicados no documento "Revisão sistemática sobre drogas na condução" (2021). Tanto assim é que a DGT afirma ajustar estes valores às recomendações internacionais mais recentes e aplicáveis, bem como às evidências geradas pela experiência espanhola neste domínio.

²² Nanograma (ng): Unidade de massa correspondente a um bilionésimo de um grama.

²³ Ver: <https://www.samhsa.gov>

²⁴ Ver: <http://www.ewdts.org>

²⁵ Ver: <https://www.nsc.org/workplace/get-involved/divisions/alcohol-drugs-impairment-division>

²⁶ Real Academia Espanhola: Organização Internacional de Normalização, o sistema internacional de normalização para a regulamentação de produtos e serviços.

²⁷ Comissão Eletrotécnica Internacional, a principal comissão de normas do mundo que desenvolve e publica normas internacionais para tecnologias electrónicas.

QUADRO 1.

Comparação dos pontos de corte analíticos para o teste de fluido oral para detecção do consumo de substâncias psicoativas em condutores da Direção-Geral de Viação e de outras organizações internacionais.

ANALITO	Limite em saliva (ng/ml)			
	EWDTS	SAMSHA	NSC-ADID	DGT
Anfetamina	15	15	15	15
Cocaína	8	8	8	8
Cetamina	10			10
MDA	15	15	15	15
MDEA	15	15		15
MDMA	15	15	15	15
Metadona	20		10	10
Metanfetamina	15	15	15	15
Morfina	15	15	5	5
THC	2	2	2	2

Fonte: Elaboração própria de acordo com a DGT (2021).
"Revisão sistemática sobre drogas e condução".

Nota: EWDTS: European Workplace Drug Testing Society (Reino Unido).
SAMSHA: Administração dos Serviços de Abuso de Substâncias e de Saúde Mental (EUA).
NSSC-ADID: National Safety Council - Alcohol, Drugs and Impairment Division (EUA).

Análise comparativa dos limites de detecção (cutoff) das substâncias a analisar no quadro 1:

5.1.1 Consenso internacional: analitos como a anfetamina, a metanfetamina, a MDMA, o MDA, a cocaína e o THC apresentam valores homogêneos (15 ng/ml para os estimulantes; 8 ng/ml para a cocaína e 2 ng/ml para o THC, o que demonstra que os padrões são amplamente aceites para a sua detecção.

5.1.2 Variabilidade em analitos específicos: A metadona e a morfina apresentam limites mais baixos no NSC-ADID e na DGT, indicando critérios mais sensíveis, possivelmente por razões forenses e de segurança rodoviária.

5.1.3 Tendência da norma da DGT: a regulamentação espanhola da DGT inclui todos os analitos relevantes, mas também adopta limites mais rigorosos em alguns casos, indicando uma prioridade da detecção precoce para fins administrativos e também de prevenção criminal.

QUADRO 2.

Comparação dos pontos de corte (positivos): DED Sotoxa²⁸, laboratório SynLab e os estabelecidos pela DGT.

ANALITO	ABBOT	SYNLAB	DGT
	SOTOXA ²⁹	Laboratório	DGT ³¹
	TOX400SEU	SYNLAB ³⁰	
6-AM (morfina) (OPI) ³²	40 ng/ml	>2,6 ng/ml	2 ng/ml
Anfetamina (AMP)	50 ng/ml	>18,8 ng/ml	15 ng/ml
Benzolecgonina (BE)	30 ng/ml	>9,9 ng/ml	8 ng/ml
Metabolito da cocaína (COC)	30 ng/ml	>10 ng/ml	8 ng/ml
Codeína (OPI)	40 ng/ml	>12,2 ng/ml	5 ng/ml
Cetamina		>12,6 ng/ml	10 ng/ml
MDA	50 ng/ml	>18,3 ng/ml	15 ng/ml
MDEA	50 ng/ml	>18,2 ng/ml	15 ng/ml
Metanfetamina (MDMA)	50 ng/ml	>18,7 ng/ml	15 ng/ml
Metadona (OPI)	40 ng/ml	>12,2 ng/ml	10 ng/ml
Morfina (OPI)	40 ng/ml	>6,2 ng/ml	5 ng/ml
Cannabis (THC)	25 ng/ml	>2,5 ng/ml	2 ng/ml

Fonte: Elaboração própria (2023); com base em relatórios da empresa comercial SYNLAB, empresa de monitorização de medicamentos e toxicologia SYNLAB.

Principais observações do quadro 2:

5.2.1 SOTOXA (DED). Apresenta os valores mais elevados e reflecte pontos de corte positivos mais permissivos, não uma concentração real.

5.2.2 SYNLAB. Comunica valores reais acima de um mínimo detetável e comunica resultados quantitativos acima de um limiar, mas não normativos.

5.1.3 DGT. Fornece os valores mais baixos e são limiares legais de confirmação toxicológica, estabelecendo os limites legais da infração administrativa e a sanção correspondente.

6. A EMPRESA DE ANÁLISES CLÍNICAS SYNLAB.

"Qualquer teste, em qualquer lugar, a qualquer hora" - este é o lema da empresa alemã Synlab Group (SYNLAB).³³

²⁸ Ver: ANEXO I. Explica a "composição e os princípios de funcionamento do analisador Abbot-SoToxa".

²⁹ Ver: <https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html>

³⁰ Extraído do relatório do ensaio de confirmação de drogas na saliva por LC-MS/MS do laboratório SYNLAB.

³¹ DGT (2021); "Systematic review on drug driving" (2021).

³² OPI: Opiáceos.

³³ Ver: <https://valenciaplaza.com/asi-es-synlab-empresa-alemana-compra-sistemas-genomicos>

A SYNLAB foi fundada em 1998 pelo Dr. Bartl Wimmer em Augsburg, juntamente com um grupo de parceiros, como uma associação de médicos de laboratório independentes. Desde então, tem crescido principalmente através de aquisições, oferecendo testes para a presença do coronavírus durante a pandemia. A SYNLAB não passou despercebida aos grandes investidores institucionais de todo o mundo, que ao longo dos anos adquiriram participações no capital da empresa. Atualmente, o principal acionista é o conhecido fundo de capital de risco britânico Cinven (também com escritório em Madrid), que detém cerca de 43% das acções, segundo as estimativas da empresa alemã. Seguem-se os dinamarqueses da Novo Holdings (17%); os canadianos do Ontario Teachers' Pension Fund (OTPP) com 8%; a mesma percentagem do fundador da SYNLAB e dos seus colaboradores próximos; e o Estado do Qatar através do seu fundo soberano (5%).

Em Espanha, a sua relação com o Ministério do Interior (de acordo com a plataforma de contratação do Setor Público do Ministério das Finanças), foi estabelecida através da DGT, que adjudicou o "serviço de determinação e quantificação de drogas e álcool em amostras de fluido oral e sangue" com base num contrato³⁴ adjudicado por um valor de 4.999.980,00 euros à SYNLAB DIAGNÓSTICOS GLOBALES S.A.U (A59845875). Para além da DGT, este laboratório clínico foi contratado por outras administrações: a Junta da Andaluzia para as análises clínicas do Centro de Prevenção de Riscos Laborais de Jaén, o Metro de Madrid e a Generalitat de Catalunya³⁵, entre outras.

7. LIMITES DE QUANTIFICAÇÃO E INTERVALOS DE INCERTEZA DOS RESULTADOS LABORATORIAIS DO SYNLAB.

Existem informações adicionais sobre as amostras de saliva apresentadas pelo laboratório SYNLAB para as substâncias acima enumeradas no quadro; é utilizado como "critério de positividade" que a concentração das substâncias seja superior ou igual aos valores do limite de quantificação (LOQ)³⁶, acrescido do "valor de incerteza" do teste; caso contrário, o resultado é negativo. Além disso, a SYNLAB refere o facto de o seu laboratório ter "a incerteza expandida para K=2 para toda a gama de trabalho".

Para clarificar o conceito de "incerteza", devemos dizer que é a "dúvida" que pode existir sobre o resultado de qualquer medição, ou seja, diz-nos sobre a fiabilidade dessa medição.

Por conseguinte, todas as medições efectuadas têm alguma "incerteza" e devem ser quantificadas para decidir se a medição efectuada é suficientemente fiável para o fim a que se destina. Além disso, deve notar-se que "erro" não é o mesmo que "incerteza", nomeadamente:

³⁴ Ver: https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfljU1JTC3Iy87KtUIJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMMyU1zLcvQj_byycwN9yy2dXPLygvNDIoyrVA3Myx1tbfULcnMdAUNYE4U!/ e BOE 97 de 23 de abril de 2019.

³⁵ Ver: <https://contractaciopublica.cat/ca/detall-publicacio/200026255>

³⁶ O termo refere-se à concentração mais baixa que pode ser atingida de forma fiável, desde que esteja dentro dos limites de precisão especificados nas operações laboratoriais de rotina.

Erro: A diferença entre o valor de medição de um dispositivo e o valor padrão ou de referência³⁷ que é considerado exato. Ao efetuar uma comparação entre valores, o erro e a incerteza são gerados de acordo com a metrologia. Assim, em conjunto, o erro e a incerteza podem ser utilizados para saber se um instrumento está dentro do erro máximo tolerado.

Incerteza³⁸ : Após efetuar várias medições durante um processo de calibração, são descobertas pequenas diferenças entre elas. Mas qual das medições é a correta, a média e o seu desvio padrão são encontrados, descobrindo qual é a diferença normal entre as medições, tornando a medição final suficientemente fiável.

Exatidão: Mede o grau de concordância entre o resultado obtido e o valor verdadeiro (ou o que é considerado como tal).

Precisão: Mostra a concordância entre duas ou mais medições efectuadas da mesma forma.

Incerteza expandida³⁹ : Antes de publicar a componente de incerteza combinada, é necessário multiplicar o resultado pelo valor sigma selecionado para obter o nível de confiança necessário. Após a multiplicação, o resultado é a incerteza expandida, ou seja, a incerteza com um determinado nível de confiança incluído.

Avaliação da incerteza K=2: A calibração é efectuada por um laboratório autorizado (calibração externa) e os dados relativos à incerteza expandida são apresentados em %, em que K=2 corresponde aproximadamente a um nível de confiança de 95 %.

Por conseguinte, podemos afirmar que os resultados analíticos das drogas salivares do laboratório SYNLAB têm um nível de confiança ou uma exatidão esperada que ronda o intervalo/limite de 95%.

8. O LABORATÓRIO SYNLAB E A SUA ACREDITAÇÃO PELO ORGANISMO NACIONAL DE ACREDITAÇÃO ATRAVÉS DE AUDITORIAS.

O Organismo Nacional de Acreditação (ENAC G-78373214 - C/Serrano 240, 4ª A-B, 28016 Madrid) é o único organismo designado pelo Governo para operar em Espanha como Organismo Nacional de Acreditação⁴⁰, regulando o funcionamento da acreditação na Europa, que se baseia em cinco princípios fundamentais: "Sem fins lucrativos, independência, não concorrência, avaliação internacional e reconhecimento mútuo"⁴¹. Além disso, o ENAC pode assinar acordos de colaboração com a Administração Geral

³⁷ Padrão, com a maior precisão disponível num determinado local ou numa determinada organização, e a partir do qual as medições são derivadas.

³⁸ NSGT (2012) Incerteza de um resultado de medição, expressa como um desvio padrão experimental. Ver: <https://www.insst.es/documents/94886/326879/930w.pdf/f657c677-ebab-4f99-8474-667d73e22882>

³⁹ INSGT (2012): Quantidade que define um intervalo em torno do resultado de uma medição, e no qual se espera encontrar uma fração significativa da distribuição de valores que poderiam ser razoavelmente atribuídos à mensuranda.

⁴⁰ RD 1715/2010 BOE 7 de núm. 7 de 8 de janeiro de 2011, "(...) em conformidade com o disposto no Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93.

⁴¹ Ver: <https://www.innotec-laboratorios.es/que-es-la-acreditacion-enac/>

do Estado e com as Administrações das Comunidades Autónomas, conforme adequado para o melhor desempenho das suas actividades e funções⁴².

A "acreditação" da ENAC deve ser uma garantia da correta execução de um determinado tipo de actividades, através de um certificado emitido por esta entidade.

A título de exemplo, a ENAC levou a cabo as seguintes actividades

Em 2013, acreditou o Instituto de Salud Carlos III⁴³ de Investigación en enfermedades raras de acordo com a norma UNE-En ISO 15189 para a realização de análises.

Ano de 2016, "auditoria externa de acreditação das actividades de ensaio e inspeção técnica ocular" dos laboratórios criminais da Guardia Civil.⁴⁴

No ano de 2018, efectuou "serviços de auditoria" na Universidade da Corunha.⁴⁵

Ano 2022, acreditou o site⁴⁶ junto da Polícia Científica do Corpo Nacional de Polícia para a "realização de inspeções técnico-policiais em locais de crime", de acordo com a norma ISO 17020.

Ano 2023, realizou "actividades de acreditação destinadas à avaliação de laboratórios" da Universidade Complutense de Madrid.⁴⁷

Por outro lado, em relação às actividades de um laboratório privado (como o SYNLAB), estas podem ser: entidades de ensaio, calibração, inspeção, certificação ou verificação, entre outras, no entanto, qualquer atividade que tenha como objetivo avaliar se um produto, serviço, sistema, instalação, etc. deve estar em conformidade com determinados requisitos pode ser objeto de acreditação.

Estes requisitos podem ser estabelecidos por lei e, por conseguinte, ter um estatuto regulamentar, ou ser legislados em normas, especificações ou outros documentos voluntários. A acreditação ENAC não só permite a qualquer laboratório ou empresa avaliada saber se a sua atividade está a ser realizada corretamente, como também garante a máxima eficiência dos seus serviços aos clientes desses laboratórios.

Para avaliar o funcionamento correto do laboratório, estão previstas auditorias anuais de acompanhamento e uma auditoria de reavaliação de quatro em quatro anos. As auditorias de acompanhamento verificam se houve alterações nos procedimentos, aquisição de novo equipamento, etc.

⁴² BOE n.º 7 de 8 de janeiro de 2011.

⁴³ Ver: https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_S DG_IIER_sin_anexo_tecnico.pdf

⁴⁴ Ver: https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_S DG_IIER_sin_anexo_tecnico.pdf

⁴⁵ Ver: https://www.udc.es/export/sites/udc/contratacionadministrativa/contratos-menores/publicar-Disp-adic-54.xls_2063069239.xls

⁴⁶ Ver: <https://www.enac.es/actualidad/policia-cientifica-inspeccion-ocular>

⁴⁷ Ver:⁴⁷ <https://www.ucm.es/file/208-2023-enac-1->

Em suma, o que o ENAC pode avaliar e certificar é o cumprimento correto da norma⁴⁸ UNE-EN ISO/IEC 17025 nesse ano. A título informativo, nas auditorias de reavaliação, todos os pontos da norma durante os quatro anos anteriores são revistos de forma mais exaustiva. Se o laboratório não cumprir os requisitos em qualquer uma destas auditorias, a acreditação pode ser suspensa.

A título informativo, as auditorias de reavaliação analisam de forma mais exaustiva todos os pontos da norma durante os quatro anos anteriores. Se o laboratório não cumprir os requisitos em qualquer uma destas auditorias, a acreditação pode ser suspensa.

⁴⁸ BOE 19 de 22 de janeiro de 2018 - Publicação pelo Ministério da Economia, Indústria e Competitividade dos "Requisitos gerais para a competência dos laboratórios de ensaio e calibração (ISO/IEC 17025:2017)".

9. TABELA 3. ÂMBITO DA ACREDITAÇÃO ⁴⁹ ENAC N° 1169/LE2347, EMITIDO PARA OS LABORATÓRIOS SYNLAB DIAGNÓSTICOS GLOBALES SA. SOBRE TESTES (REVISTO EM 23/12/2022).

ORGANISMO NACIONAL DE ACREDITAÇÃO (ENAC)

PRODUTO/M ATERIAL A SER TESTADO	ESSAIO	NORMA / PROCEDIMENTO DE ENSAIO																																																																					
<i>PRODUTOS/M ATERIAIS TESTADOS</i>	<i>TIPO DE ENSAIO</i>	<i>ESPECIFICAÇÕES NORMALIZADAS/PRO CEDIMENTO DE ENSAIO</i>																																																																					
Saliva (direta ou saliva em tampão) Sangue total	Determinação quantitativa de substâncias de abuso por cromatografia líquida de alta resolução ultra-rápida com detecção por espetrometria de massa em tandem.	Procedimento interno LCMS-004 Rev.15 LCMS-0010 Rev.9																																																																					
<i>Saliva (direta ou saliva em tampão) Sangue</i>	LOQ⁵⁰ ng/ml LOQ ng/ml <table> <tr> <th>SUBSTÂNCIA</th><th>Saliva</th><th>Sangue</th></tr> <tr> <td>Morfina</td><td>1</td><td>1</td></tr> <tr> <td>Codeína</td><td>1</td><td>2</td></tr> <tr> <td>Heroína</td><td>2</td><td>2</td></tr> <tr> <td>Anfetamina</td><td>1</td><td>2</td></tr> <tr> <td>Metanfetamina</td><td>1</td><td>2</td></tr> <tr> <td>MDA</td><td>2</td><td>2</td></tr> <tr> <td>MDMA</td><td>2</td><td>2</td></tr> <tr> <td>MDEA</td><td>2</td><td>2</td></tr> <tr> <td>Cocaína</td><td>1</td><td>2</td></tr> <tr> <td>Metadona</td><td>2</td><td>2</td></tr> <tr> <td>Cetamina</td><td>2</td><td>2</td></tr> <tr> <td>LSD</td><td>2</td><td>2</td></tr> <tr> <td>Clonazepam</td><td>2</td><td>2</td></tr> <tr> <td>Alprazolam</td><td>2</td><td>2</td></tr> <tr> <td>Diazepam</td><td>1</td><td>2</td></tr> <tr> <td>Lorazepam</td><td>2</td><td>2</td></tr> <tr> <td>Oxazepam</td><td>2</td><td>2</td></tr> <tr> <td>Nordiazepam</td><td>1</td><td>2</td></tr> <tr> <td>Tramadol</td><td>1</td><td>2</td></tr> <tr> <td>Fenciclidina</td><td>2</td><td>2</td></tr> <tr> <td>Dextropropoxifeno</td><td>1</td><td>2</td></tr> <tr> <td>Zolpidem</td><td>1</td><td>2</td></tr> </table>	SUBSTÂNCIA	Saliva	Sangue	Morfina	1	1	Codeína	1	2	Heroína	2	2	Anfetamina	1	2	Metanfetamina	1	2	MDA	2	2	MDMA	2	2	MDEA	2	2	Cocaína	1	2	Metadona	2	2	Cetamina	2	2	LSD	2	2	Clonazepam	2	2	Alprazolam	2	2	Diazepam	1	2	Lorazepam	2	2	Oxazepam	2	2	Nordiazepam	1	2	Tramadol	1	2	Fenciclidina	2	2	Dextropropoxifeno	1	2	Zolpidem	1	2	
SUBSTÂNCIA	Saliva	Sangue																																																																					
Morfina	1	1																																																																					
Codeína	1	2																																																																					
Heroína	2	2																																																																					
Anfetamina	1	2																																																																					
Metanfetamina	1	2																																																																					
MDA	2	2																																																																					
MDMA	2	2																																																																					
MDEA	2	2																																																																					
Cocaína	1	2																																																																					
Metadona	2	2																																																																					
Cetamina	2	2																																																																					
LSD	2	2																																																																					
Clonazepam	2	2																																																																					
Alprazolam	2	2																																																																					
Diazepam	1	2																																																																					
Lorazepam	2	2																																																																					
Oxazepam	2	2																																																																					
Nordiazepam	1	2																																																																					
Tramadol	1	2																																																																					
Fenciclidina	2	2																																																																					
Dextropropoxifeno	1	2																																																																					
Zolpidem	1	2																																																																					



Fonte: SYNLAB (Elaboração própria)

⁴⁹Ver: https://synlab.es/fileadmin/user_upload/Calidad_docs/Anexo_Tecnico_ISO_17025_version_7.pdf

⁵⁰ LOQ: Limite de quantificação ou nível mais baixo.

PRINCIPAIS OBSERVAÇÕES DO QUADRO 3:

9.1. AUMENTO DA SENSIBILIDADE DA SALIVA.

Para quinze das vinte e duas substâncias constantes do quadro, o LOQ na saliva é inferior ao do sangue, o que realça a eficácia desta matriz na deteção precoce da substância.

9.2. SENSIBILIDADE IGUAL NAS MATRIZES PARA DETERMINADOS COMPOSTOS.

Sete substâncias (por exemplo, LSD, cetamina, benzodiazepinas) têm o mesmo LOQ em ambas as matrizes (2 ng/ml), indicando que a matriz não afecta significativamente a sensibilidade analítica para estes compostos.

9.3. POSSÍVEIS IMPLICAÇÕES CLÍNICAS E FORENSES.

A saliva estabeleceu-se como uma alternativa não invasiva e altamente sensível para a análise toxicológica, de tal modo que o LOQ mais baixo da saliva favorece a sua utilização em contextos como: pontos de controlo de drogas, programas de desintoxicação ou monitorização ocupacional, em que o acesso a um teste sanguíneo pode ser limitado e pouco operacional.

9.4. ANÁLISE SALIVAR VS. ANÁLISE SANGUÍNEA.

A saliva posicionou-se como uma matriz de elevado valor em toxicologia analítica, não só devido à sua menor invasividade, mas também devido à sua capacidade de oferecer níveis mais elevados de sensibilidade para a deteção rápida de consumos recentes.

A deteção precoce é particularmente relevante em situações de prevenção e controlo em tempo real, tanto nos pontos de controlo de drogas como em acidentes rodoviários que envolvam um condutor sob a possível influência destas substâncias.

A utilização da saliva, em combinação com a análise laboratorial, representa um instrumento analítico eficaz com uma sensibilidade superior à do sangue. Isto em termos de limite de quantificação para um amplo espectro de substâncias de abuso.

A recomendação de incorporar a análise salivar como matriz de referência nos protocolos de deteção precoce e no diagnóstico toxicológico moderno provou ser correta.

10. CONCLUSÕES.

Primeiro. As Nações Unidas instam os governos e as instituições (públicas e privadas), através da aplicação da legislação em matéria de VS, a reduzir o número de mortes na estrada relacionadas com a droga.

Em segundo lugar. Em Espanha, a DGT (Ministério do Interior) estabeleceu uma política de "tolerância zero" ao volante, classificando a condução com a presença de drogas no organismo como um comportamento de risco. Este comportamento é sempre punido, quer como infração administrativa, quer como infração penal.

Em terceiro lugar. Apesar da ausência de acordos internacionais sobre "pontos de corte", a DGT estabeleceu o "ponto de corte" das quantidades psicoactivas mínimas. Estas quantidades estão em conformidade com as de organizações públicas e privadas tanto na UE como nos EUA. Deste modo, a DGT determinou a positividade quantitativa de qualquer droga consumida recentemente por um condutor, que será depois analisada no laboratório de referência.

Quarto. A doutrina da FGE sustenta o procedimento de recolha de amostras salivares após o teste circunstancial positivo, através de: formação específica dos agentes na recolha da amostra, garantia da cadeia de custódia e posterior análise salivar em laboratório de referência.

Quinto. O TC mantém o art. 14º da LSV, esclarecendo que a Lei não proíbe o consumo de drogas; o que proíbe é a condução com a presença de drogas no organismo.

Sexto. O TC equipara e coloca no mesmo patamar o risco que um condutor que tenha consumido drogas, mesmo as consumidas sob prescrição médica, pode gerar para o SV.

Sétimo. Os "pontos de corte" do DED portátil (SoToxa Abbott) utilizado para efetuar o primeiro "teste índice", duplicam ou triplicam os "pontos de corte" de referência efectuados pelo laboratório SYNLAB.

Oitavo. Os "pontos de corte" do laboratório clínico SYNLAB são mais elevados do que os determinados pela norma ISO, que a DGT aplica para estabelecer as quantidades psicoactivas mínimas nos aparelhos de análise laboratorial.

Nono. A aprovação das análises clínicas salivares do laboratório SYNLAB é avalizada pela Entidade Nacional de Acreditação (ENAC), que certifica o cumprimento da norma UNE do equipamento e do procedimento utilizado pelo laboratório SYNLAB na obtenção de diagnósticos salivares, tanto no tipo de droga detectada como na sua quantidade.

Décimo. A avaliação do equipamento e do procedimento de obtenção da análise das amostras de saliva do laboratório SYNLAB pela ENAC, acredita o nível de confiança ou precisão de 95% dos resultados finais obtidos e reflectidos no seu relatório final.

11. REFERÊNCIAS.

- Abade. (2020). Analisador portátil de testes toxicológicos SoToxa. https://www.tecmedica.es/cmsAdmin/uploads/o_1f24002cp1ieo17701uni19v4vaja.pdf.
- Abade. (2020). SoToxa Portable Oral Fluid Analyser (Manual do utilizador). <https://testdealcoholhydrogas.cl/wp-content/uploads/2022/08/Manual-APOC0798-v2.a-SoToxa-Mobile-Analyser-User-Guide-FWO-LA.pdf>
- Associação Espanhola de Normalização (2017). Requisitos gerais para a competência dos laboratórios de ensaio e calibração (ISO/IEC 17025:2017). <https://www.une.org/>
- Bequir, S. (2020). Teste de drogas na saliva, quanto tempo dura? <https://institutocastelao.com/test-de-droga-en-saliva/>
- Calafat, A et al. (2002). A vida recreativa nocturna dos jovens espanhóis como fator de risco em relação a outros mais tradicionais. <https://www.redalyc.org/pdf/2891/289122037002.pdf>
- Certum Diagnostics (2019). Teste de despistagem de drogas (urina). https://industriasquimicasybiologicas.com/wp-content/uploads/2020/09/Brochure-cassete-individualPrueba-de-Drogas-Certum_Kabla.pdf
- Direção-Geral do Tráfico (2021). Revisão sistemática sobre drogas e condução. <https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistemica-sobre-drogas-y-conduccion>
- Direção Geral de Tráfego (2022). Estratégia de Segurança Rodoviária 2030. <https://seguridadvial2030.dgt.es/inicio/>
- Entidad Nacional de Acreditación (n.d.). Brochura institucional da ENAC. <https://www.enac.es/actualidad/material-multimedia>
- Organismo Nacional de Acreditação (2022). Relatório 2022. <https://www.enac.es/memoria-2022>
- Procuradoria-Geral da República (2021). Circular 10/2011 FGE, de 17 de novembro, sobre os critérios da unidade de ação especializada da Procuradoria-Geral da República em matéria de segurança rodoviária. <https://www.boe.es/buscar/doc.php?id=FIS-C-2011-00010>
- Instituto Nacional de Toxicologia (2021). Tabela de doses psicoactivas mínimas das principais substâncias tóxicas traficadas. https://pnsd.sanidad.gob.es/ciudadanos/legislacion/delitos/pdf/20210730_INTF_dosis_minimas_psicoactivas_trafico_de_drogas.pdf
- Observatório Espanhol da Droga e das Toxicodependências (2023). Relatório 2023 - Álcool, Tabaco e Drogas Ilícitas em Espanha.

<https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/informesEstadisticas/pdf/2023OEDA-INFORME.pdf>

Observatório Nacional de Segurança Rodoviária. (2021). Revisão sistemática sobre drogas e condução. <https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistemica-sobre-drogas-y-conduccion>

Organização Mundial de Saúde. (2021). Plano Global - Década de Ação para a Segurança Rodoviária 2021-2030. <https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030>

Ortega Matus, M. (2022). Anticorpos monoclonais e sua utilização para identificar morfina em fluidos biológicos. <https://riiad.org/index.php/riiad/article/view/riiad-2023-1-09/389>

Parra, M. & Vega, V. (2021). Análise de drogas de abuso no laboratório clínico. <https://www.seqc.es/download/tema/38/7601/85888673/142010/cms/tema-9-analisis-de-drogas-de-abuso-en-el-laboratorio-clinico.pdf/>

Ramírez, J. (2024). Los controles de drogas a conductores en España. <https://observatoriocannabis.com/wp-content/uploads/2024/10/controlesdedrogas.pdf>

Ruiz Viera, L. (2018). Anticorpos monoclonais terapêuticos. <https://riull.ull.es/xmlui/bitstream/handle/915/12352/Anticuerpos+monoclonal+therapeutic.pdf;jsessionid=3462A6DCEAB9DA8E32233B47C6D926E0?sequence=1>

GSC-Laboratories (2023). Como avaliar a incerteza de medição sem ser um especialista em matemática. <https://sgc-lab.com/guia-para-estimar-la-incertidumbre-de-la-medicion-hecha-para-personas-normales/>

ANEXO I

COMPOSIÇÃO E PRINCÍPIOS DO ANALISADOR ABBOT-SOTOXA

1.1. COMPOSIÇÃO.⁵¹

O analisador Abbot SoToxa é composto por um sistema de analisador portátil (DED), um cartucho ou kit de teste e um dispositivo de recolha de fluido oral.

1.1.1. O analisador:

Trata-se de um dispositivo portátil de teste digital de saliva, que utiliza algoritmos para determinar a intensidade das linhas de contraste (que aparecerão na tira do cartucho de teste após todo o processo) e que também pode apresentar num ecrã e imprimir os resultados qualitativos e nominativos das drogas detectadas.

1.1.2 O cartucho de ensaio:

Composto por uma tira de imunoensaio⁵² chromatographic⁵³ rápida descartável de utilização única, contendo reagentes secos e uma solução tampão. Este kit é introduzido no analisador que o aquece à temperatura óptima para o teste.

1.1.3 O dispositivo de recolha:

Trata-se de um dispositivo descartável que recolhe o fluido oral (saliva). Deve ser esfregado nas gengivas, na língua e no interior das bochechas até o indicador de presença ficar azul.

1.2. PROCESSO DE ENSAIO:

O fluido oral recolhido no dispositivo de colheita é combinado com a solução tampão, depois misturado e incubado antes de entrar em contacto com as tiras de imunoensaio instaladas no cartucho de teste com uma *"membrana controlada pela humidade"*.

A mistura da solução e da saliva obtida desce pelo capilar da tira de cartucho e arrasta consigo os anticorpos antidroga marcados depositados sobre ele. Na ausência de fármaco na amostra, o anticorpo liga-se à mistura fármaco-proteína, formando uma linha. Na presença de droga, a formação desta linha é mais fraca.

O DED lê então a intensidade das linhas na tira de imunoensaio do cartucho e compara essa intensidade com um limiar ou ponto de corte pré-determinado da

⁵¹ Abbott (2020); "SoToxa Portable Oral Fluid Analyser" (Manual do utilizador).

⁵² É utilizado um imunoensaio cromatográfico rápido para a deteção quantitativa de múltiplas drogas e metabolitos de drogas na saliva, fornecendo apenas um resultado analítico preliminar.

⁵³ A cromatografia é uma técnica efectuada em laboratório para separar componentes em misturas simples ou complexas. Existem muitos tipos diferentes de cromatografia, desde a cromatografia em papel e a cromatografia em camada fina até à cromatografia gasosa.

Ver: <https://www.onelab.com.ar/cromatografia-que-es-y-para-que-sirve-informacion-completa>

concentração do fármaco, obtendo um resultado qualitativo (não quantitativo). Os resultados são então apresentados no ecrã do DED e podem ser impressos.

1.3. RESULTADOS POSITIVOS.

O manual da Abbot SoToxa DED especifica que os resultados positivos obtidos devem ser confirmados por um segundo método, como a espetrometria de massa por cromatografia gasosa (GC-MS). Além disso, a DED e os seus resultados não se destinam a utilização doméstica, clínica, terapêutica ou de diagnóstico.

1.4. COMPOSIÇÃO DA TIRA DE IMUNOENSAIO DO CARTUCHO.

O conteúdo do imunoensaio de cromaticidade consiste numa tira impregnada com uma série de reagentes secos que contêm anticorpos monoclonais⁵⁴ (mAbs). Estes anticorpos (AC) são proteínas criadas em laboratório e são utilizados para identificar metabolitos de drogas de abuso em fluidos biológicos.

Os mAbs têm uma elevada sensibilidade e ligam-se, por exemplo, à morfina e aos seus metabolitos, pelo que podem ser utilizados para gerar um resultado marcado através do "rastreo" da tira de teste ou da membrana do cartucho, detectando seletivamente níveis elevados de drogas específicas na saliva.

⁵⁴ Os anticorpos monoclonais têm atualmente inúmeras aplicações, tanto na investigação biomédica como no diagnóstico e tratamento de numerosas patologias. Esta qualidade dos anticorpos monoclonais deve-se à sua elevada especificidade e à sua grande afinidade com o alvo terapêutico.



Artigo de investigação

PROTECÇÃO DAS INFRA-ESTRUTURAS SUBMARINAS CRÍTICAS E REFORÇO DA SEGURANÇA DO MAR BÁLTICO: OPERAÇÃO SENTINELA DO MAR BÁLTICO DA NATO

Tradução para o português com ajuda de IA (DeepL)

Mónica Román González

**Doutorando do Programa de Ciência Política e Administração e Relações
Internacionais da Universidade Complutense de Madrid.**

**Mestrado em Política Internacional: estudos sectoriais e de área na Universidade
Complutense de Madrid.**

monicaromangz@gmail.com

ORCID: <https://orcid.org/0009-0007-8698-3739>

Google Scholar: <https://scholar.google.com/citations?user=2-KCa2kAAAJ&hl=es&oi=sra>

Recebido em 31/03/2025

Aceite em 28/05/2025

Publicado em 27/06/2025

Citação recomendada: Román, M. (2025). A proteção das infra-estruturas críticas submarinas e o reforço da segurança do Mar Báltico: a operação Baltic Sentry da NATO. *Revista Logos Guardia Civil*, 3(2), p.p. 221-256.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

PROTECÇÃO DE INFRA-ESTRUTURAS SUBMARINAS CRÍTICAS E REFORÇO DA SEGURANÇA DO MAR BÁLTICO: OPERAÇÃO SENTINELA DO MAR BÁLTICO DA NATO

Resumo: INTRODUÇÃO. 2. ENQUADRAMENTO DO ESTUDO. 2.1. A importância geoestratégica do Mar Báltico. 2.2. A proteção das infra-estruturas submarinas críticas. 2.3. A situação das infra-estruturas submarinas críticas no mar Báltico desde o início da invasão total da Ucrânia pela Rússia em 2022. A NATO E A PROTECÇÃO DAS INFRA-ESTRUTURAS SUBMARINAS CRÍTICAS. 4. OPERAÇÃO SENTINELA DO BÁLTICO. 5. CONCLUSÕES E PROPOSTAS. 6. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: Os danos causados aos cabos submarinos no Mar Báltico têm feito soar os alarmes sobre o potencial de guerra híbrida e a vulnerabilidade das infra-estruturas submarinas críticas ocidentais à sabotagem, sendo os repetidos incidentes na área um dos principais exemplos das tensões geopolíticas existentes atualmente. O principal objetivo deste artigo é analisar a Operação *Baltic Sentry* da NATO no contexto da crescente necessidade da Aliança Atlântica em assegurar a proteção deste tipo de infra-estruturas críticas no estratégico Mar Báltico e assim reforçar a segurança deste último. Recorrendo a métodos de investigação mistos, este artigo começa por explicar a importância da proteção de infra-estruturas submarinas críticas no Mar Báltico, de importância geoestratégica, e descreve o quadro geral da OTAN para a proteção dessas infra-estruturas. Em seguida, o estudo apresenta as principais características da Operação *Baltic Sentry*, lançada pela NATO em janeiro de 2025, concluindo que a mesma reúne as necessidades necessárias para ser uma boa estratégia capaz de permitir à Aliança progredir na concretização de dois dos seus principais objectivos prioritários: a proteção de infra-estruturas cada vez mais importantes, como as infra-estruturas submarinas críticas, e o consequente reforço da segurança no Mar Báltico, de forma a garantir a sua resiliência.

Resumen: Los daños sobre los cables submarinos en el Mar Báltico han encendido las alarmas sobre una potencial guerra híbrida y la vulnerabilidad de las infraestructuras críticas submarinas occidentales ante posibles sabotajes, siendo así los reiterados incidentes sobre la zona señalada uno de los principales ejemplos de las tensiones geopolíticas existentes en la actualidad. El presente artículo tiene como principal objetivo analizar la Operación *Baltic Sentry* de la OTAN en un contexto en el que impera la creciente necesidad de la Alianza Atlántica de asegurar la protección de este tipo de infraestructuras críticas en el estratégico Mar Báltico y de reforzar así la seguridad sobre este último. Para ello, a través del empleo de métodos mixtos de investigación, el presente artículo primero explica la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico para después exponer el marco general de acción de la OTAN respecto a la protección de estas infraestructuras. Tras ello, el estudio expone las principales características de la Operación *Baltic Sentry* lanzada por la OTAN en enero de 2025 concluyendo que esta se ajusta a las necesidades requeridas para ser una buena estrategia capaz de permitir a la Alianza avanzar en la consecución de dos de sus principales objetivos prioritarios: la protección de unas infraestructuras cuya importancia es cada vez

mayor como son las infraestructuras críticas submarinas y el consiguiente refuerzo de la seguridad en el Mar Báltico en pro de garantizar su resiliencia.

Palavras-chave: Organização do Tratado do Atlântico Norte (NATO), Mar Báltico, infra-estruturas submarinas críticas, segurança, Baltic Sentry.

Palabras clave: Organización del Tratado del Atlántico Norte (OTAN), Mar Báltico, infraestructuras críticas submarinas, seguridad, Baltic Sentry.

ABREVIATURAS

CCD COE: *Centro de Excelência Cooperativo de Ciberdefesa*

CCOE: *Centro de Excelência de Cooperação Civil-Militar*

CMRE: *Centro de Investigação e Experimentação Marítima da NATO*

CONVEMAR: *Convenção das Nações Unidas sobre o Direito do Mar*

RRC: *Currículo de Referência para a Resiliência*

CTF: *Comandante da Task Force*

GNL: *Gás Natural Liquefeito*

GUGI: *Glavnoye upravlenie glubokovodnikh issledovaniy* ou *Direção Principal de Investigação da Profundidade do Mar*

MARCOM: *Comando Marítimo Aliado* ou *Comando Naval da NATO no Reino Unido*

NATO: *Organização do Tratado do Atlântico Norte*

NSC: *Centro de Expedição da NATO*

NATO: *Organização do Tratado do Atlântico Norte*

SOFCOM: *Comando das Forças Aliadas de Operações Especiais*

UE: *União Europeia*

URSS: *União das Repúblicas Socialistas Soviéticas*

USV: *Veículo de superfície não tripulado*

ZEE: *Zona Económica Exclusiva*

1. INTRODUÇÃO

Nos últimos tempos, a importância das infra-estruturas submarinas críticas aumentou drasticamente, uma vez que facilitam a prestação de serviços básicos como a energia, as transacções financeiras, as comunicações ou a Internet. Isto faz com que a vulnerabilidade destas infra-estruturas seja uma das principais preocupações dos actores internacionais, especialmente tendo em conta que o controlo dos fundos marinhos continua a emergir como um elemento determinante nas relações de poder deste século (Conte de los Ríos, 2025, p. 34). Se, por um lado, a recente proliferação da tecnologia submarina e a consequente aquisição da capacidade de conduzir operações sofisticadas favoreceram as suas capacidades de protecção, por outro lado, tais inovações oferecem um leque de possibilidades aos actores que pretendam explorar as suas fragilidades (Cassetta, 2024, p. 2).

Neste sentido, qualquer ataque à infraestrutura submarina da Organização do Atlântico Norte (NATO) teria graves consequências para a segurança dos seus Estados membros, tornando-a um alvo para os seus rivais. Tendo em conta que um ataque a estes cabos requer a disponibilidade de meios precisos, a Rússia e, em menor escala, a China são os países que podem ser identificados como a ameaça mais direta, de acordo com o Insikt Group (2023, p. 11-15) no seu último relatório sobre os riscos para os cabos submarinos.

Assim, a chamada "guerra dos fundos marinhos", mais vulgarmente conhecida por *Seabed Warfare*, é atualmente uma ameaça imediata para a Aliança Atlântica. Episódios como os repetidos incidentes envolvendo cabos submarinos no geoestratégico Mar Báltico evidenciam a magnitude dos riscos colocados por uma ameaça que exige esforços e investimentos coordenados para complementar as estratégias concebidas por cada Estado. É aqui que entra em jogo a nova operação da OTAN para proteger as infra-estruturas submarinas críticas no Mar Báltico - a Operação *Baltic Sentry*.

Existe uma vasta literatura sobre esta questão. Por um lado, as principais razões que explicam a importância da protecção das infra-estruturas críticas submarinas são amplamente abordadas em investigações de especialistas na matéria, como Noelia Arjona Hernández (2023), Rafael García Pérez (2024) e Augusto Conte de los Ríos (2025). Por outro lado, no que diz respeito ao papel da NATO na protecção destas infra-estruturas, destacam-se o relatório de Njall Trausti Fridbertsson (2023) ou o artigo de Sean Monaghan, Otto Svendsen, Michael Darrah e Ed Arnold para o *Center for Strategic & International Studies* (2023). Assim sendo, o objetivo geral deste estudo é analisar a recentemente anunciada Operação *Baltic Sentry* no quadro da NATO para o reforço da segurança do Mar Báltico através da protecção de infra-estruturas submarinas críticas.

Assim, a questão geral de investigação que orienta este estudo é: Como é que a Operação *Baltic Sentry* da NATO responde à protecção de infra-estruturas submarinas críticas no Mar Báltico? A hipótese geral da investigação é que a Operação *Baltic Sentry* melhora a protecção das infra-estruturas submarinas críticas no Mar Báltico e a presença da Aliança no Mar Báltico, ajustando-se assim ao novo ambiente de ameaça.

Para o efeito, foram definidos dois objectivos específicos. Primeiro, explicar a importância da protecção das infra-estruturas críticas submarinas numa área de grande relevância geoestratégica como o Mar Báltico, especialmente no atual contexto internacional marcado pela ameaça russa após a sua invasão da Ucrânia e pelo aumento dos danos sofridos por este tipo de infra-estruturas desde então. Em segundo lugar, definir

o quadro geral de atuação da NATO no que respeita à proteção das infra-estruturas críticas submarinas.

Assim, tendo utilizado métodos de investigação mistos, o estudo conclui com conclusões relativas ao novo projeto da NATO, na medida em que tenta abordar duas questões de segurança cada vez mais importantes: a proteção de infra-estruturas submarinas críticas e o consequente reforço da segurança do Mar Báltico.

2. ENQUADRAMENTO DO ESTUDO

2.1. A IMPORTÂNCIA GEOESTRATÉGICA DO MAR BÁLTICO

Localizado no norte da Europa (ver Figura 1), o Mar Báltico tem sido historicamente uma área de competição geopolítica, que agora reemergiu como um ponto crucial de ameaça à segurança europeia após a invasão da Ucrânia. Para além dos seus benefícios comerciais e em termos de recursos marinhos, este enclave é um pólo fundamental para infra-estruturas que contribuem significativamente para o abastecimento energético de vários Estados europeus, eles próprios membros da NATO (Fridbertsson, 2023, p. 2).

A própria Aliança define-o como "um centro vital para o comércio e o transporte de energia que liga numerosas nações aliadas", sendo um canal para o fornecimento de energia e um suporte para cabos submarinos que transferem dados, dois elementos cruciais para a economia e a segurança dos Aliados (NATO Allied Maritime Command, 2025a).

Figura 1
Mapa político do Mar Báltico.



Fonte: McNamara (2016).

Com a adesão da Finlândia e da Suécia à NATO em 2023 e 2024, o Mar Báltico passou a ser conhecido como "o lago da NATO". No entanto, este rótulo não é suficientemente adequado, tendo em conta que os Aliados na região ainda enfrentam

inúmeras ameaças e, tal como definido por John Deni (2023), um cenário de segurança regional dinâmico que os obriga a unir forças através dos diferentes quadros de cooperação à sua disposição. Esta situação decorre principalmente da presença da Rússia na região, que coloca desafios crescentes à segurança dos Aliados, especialmente no contexto atual que torna a proteção do chamado flanco oriental da NATO uma questão de segurança prioritária.

Historicamente, a Rússia tem sido um ator importante na região do Báltico. Por um lado, tem a cidade portuária de São Petersburgo, um importante centro económico e cultural do país, por onde passa a maior parte do seu comércio marítimo desde o tempo de Pedro, o Grande. Por outro lado, a Rússia controla também o enclave de Kaliningrado, entre a Polónia e a Lituânia, onde tem bases militares com a Frota do Báltico (Savitz e Winston, 2024, p. 5).

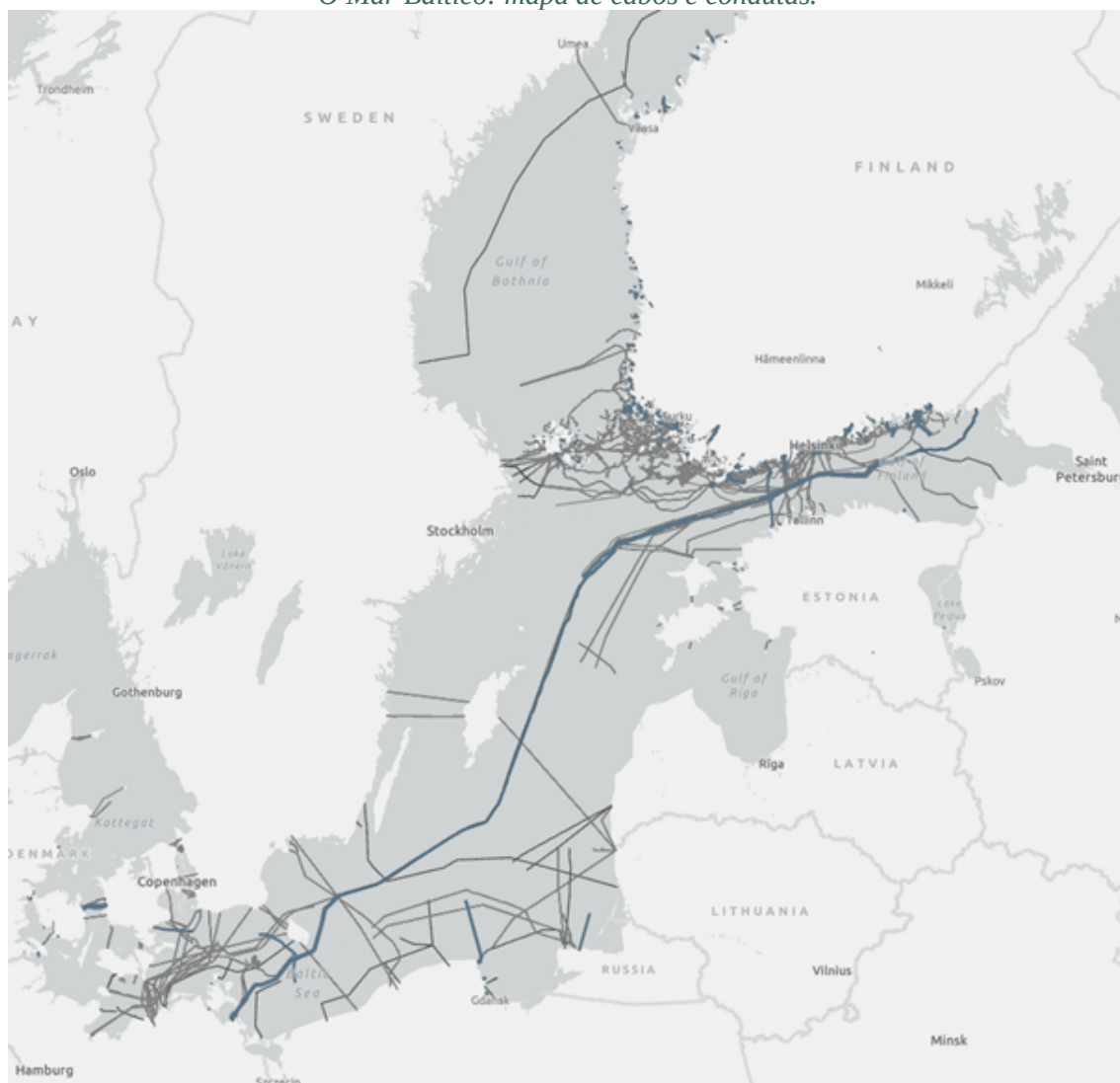
Além disso, a chamada "Frota Fantasma Russa", uma frota de navios-tanque criada pelo Kremlin que navega sob bandeiras de outras nações para escapar às sanções impostas após a sua agressão ilegal contra a Ucrânia, está atualmente a operar no Mar Báltico (Childs, 2025, p. 5). Tal como outros navios russos, este está equipado com tecnologia capaz de monitorizar o fundo do mar e, por isso, é também suspeito de participar na campanha híbrida da Rússia contra o Ocidente através da recolha de informações e da subsequente preparação de sabotagem de infra-estruturas submarinas críticas (Jones, 2025, p. 8). A isto acresce o facto de Moscovo ter demonstrado repetidamente as suas ambições expansionistas sobre uma região que poderia ser o seu próximo alvo, especialmente no auge da sua hostilidade para com a NATO.

Consequentemente, a Rússia é o principal desafio para a Aliança na região. Na região, Moscovo encontra nas táticas híbridas o principal instrumento de pressão sobre os aliados para atenuar as fraquezas militares convencionais e minimizar os riscos de provocar um confronto direto entre as partes (Cassetta, 2024, p. 2). Como é sabido, as sabotagens são executadas de forma a dificultar a identificação dos responsáveis, levando os países envolvidos a serem cautelosos na atribuição de responsabilidades por receio de uma escalada. Assim, são úteis à Rússia para minar a NATO, impedindo a ativação do artigo 5º da defesa colectiva (Jones, 2025, p. 3).

Ao mesmo tempo, vale a pena notar que as capacidades submarinas da Rússia são a sua principal força para competir na região. Como explica Sidharth Kaushal (2023), Moscovo tem a Direção Principal para a Investigação em Águas Profundas (*Glavnoye upravlenie glubokovodnikh issledovaniy*, GUGI), uma agência secreta sob a alçada do Ministério da Defesa russo que opera submarinos e navios capazes de se envolver em sabotagem.

Considerando que as capacidades de ataque a infra-estruturas críticas da Rússia são uma componente fundamental da sua estratégia (Fink e Kofman, 2020, p. 16), poderiam ser utilizadas para intercetar comunicações críticas na região do Báltico (Metrick e Hicks, 2018, p. 7). Esta região alberga uma complexa rede de infra-estruturas submarinas que é fundamental para a comunicação e o fornecimento de energia entre as nações europeias (ver Figura 2).

Figura 2
O Mar Báltico: mapa de cabos e condutas.



Fonte: Comissão de Proteção do Meio Marinho do Báltico (2024).

A proteção destas infraestruturas marítimas críticas nesta região geoestratégica chave depende fortemente da NATO (Fridbertsson, 2023, p. 11), o que abre uma janela de oportunidade para Moscovo no seu desejo de enfraquecer o Ocidente.

2.2. PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS SUBAQUÁTICAS

As comunicações, as transacções financeiras, a energia e uma vasta gama de actividades diárias essenciais dependem de infra-estruturas submarinas críticas. De acordo com os dados fornecidos pelo *Submarine Telecoms Forum* (2025, p. 8-9) no seu último relatório, 99% do tráfego internacional de dados transita por cabos submarinos, o que os torna "a espinha dorsal das comunicações mundiais".

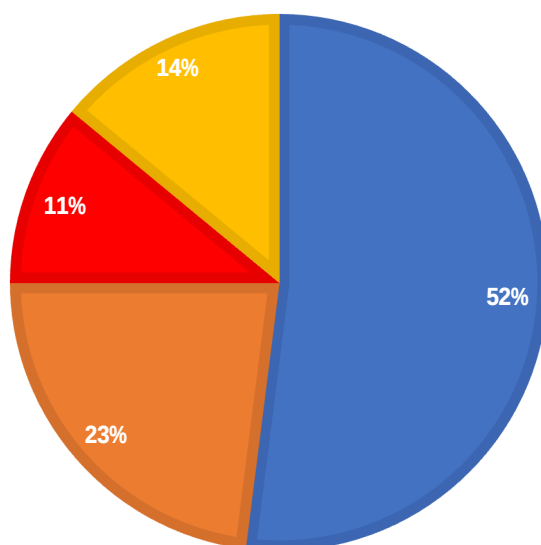
A sua importância é tal que qualquer dano pode ter consequências graves para a estabilidade da sociedade, o que torna a sua segurança de importância geoestratégica fundamental, tornando-a um bem inestimável cuja proteção deve ser uma prioridade nas agendas de segurança (Quijarro Santibáñez, 2023, p. 15-22) (Fridbertsson, 2023, p. 2) (García Pérez, 2024, p. 265-298).

A crescente dependência das infra-estruturas críticas submarinas e a atual convergência de ameaças tradicionais e emergentes fazem da sua proteção um dos maiores desafios em matéria de segurança (Conte de los Ríos, 2025, p. 26), especialmente dada a sua vulnerabilidade a ameaças naturais e de origem humana (Guilfoyle, Paige e McLaughlin, 2022, p. 657-696). O *International Cable Protection Committee* (2024, p. 5) argumenta que a interação humana é a causa mais comum de danos nos cabos, geralmente causados pela pesca e por âncoras (ver Figura 3).

Figura 3

Gráfico das principais causas de rupturas/quebras de cabos de acordo com o Comité Internacional de Proteção de Cabos.

■ Pesca ■ Âncoras ■ Terceiros ■ Sem terceiros



Fonte: Comité Internacional de Proteção dos Cabos (2024, p. 5).

Já em 2016, face ao aumento da atividade submarina russa a um nível não conhecido desde a Guerra Fria, James Foggo e Alarik Fritz (2016) propuseram a sua ideia da existência de "A Quarta Batalha do Atlântico", na qual as infra-estruturas submarinas, em particular as plataformas de abastecimento de energia e os cabos de telecomunicações, seriam ameaçadas. Uma batalha que, segundo James Foggo (2023), começou a sério após o aparente ataque ao gasoduto Nord Stream em 2022.

O facto é que a importância destas infra-estruturas tornou-as não só um alvo prioritário de proteção, mas também um alvo possível de ataques por parte de actores interessados em desestabilizar outros. Incidentes como o acima referido sensibilizaram para as vulnerabilidades destas infra-estruturas no contexto das tensões internacionais, o que constituiu um ponto de viragem no entendimento de que a adoção de medidas que garantam a sua proteção é fundamental (Fridbertsson, 2023, p. 11) (Monaghan et al., 2023, p. 2).

Por outro lado, a constante evolução tecnológica acarreta importantes repercussões ao nível das capacidades submarinas que os diferentes atores devem adquirir (Clark, 2015, p. 18), algo que tem contribuído significativamente para a consolidação do

domínio submarino como o chamado "sexto domínio". Este novo domínio operacional, cada vez mais disputado, concentra interesses económicos, estratégicos e militares devido à riqueza de recursos que alberga e que o tornam um teatro de conflito conhecido como *Seabed Warfare* (Conte de los Ríos, 2025, pp. 29-30). Embora a sua concetualização ainda esteja a ser desenvolvida por actores como a NATO, Conte de los Ríos (2025, p. 29) define-a como o conjunto de operações realizadas no, para, de, sobre e sob o fundo do mar com fins estratégicos ou militares, utilizando como caso representativo a sabotagem do gasoduto Nord Stream.

O domínio marítimo é particularmente vulnerável às ameaças híbridas. Para além do facto de estas últimas serem difíceis de distinguir dos danos acidentais, os agressores podem utilizar a cobertura de embarcações de vários tipos difíceis de rastrear, tais como navios de pesca ou embarcações privadas (Monaghan et al., 2023, p. 6). A este respeito, convém recordar que, uma vez que a sabotagem não é considerada uma violação da proibição do uso da força ao abrigo da Carta das Nações Unidas, o direito internacional restringe a resposta militar aos danos nos cabos, especialmente quando estão envolvidos navios não militares (Conte de los Ríos, 2023, p. 33).

Christian Bueger e Tobias Liebetrau (2021) argumentam que a governação das infra-estruturas críticas subaquáticas é mais complexa devido a dois factores: (1) a necessidade de cooperação internacional por parte de vários actores estatais - que agem com base nos seus benefícios estratégicos - e (2) o facto de parte destas infra-estruturas ser propriedade do sector privado - cujo papel é relevante, tendo em conta que os seus interesses podem estar desalinhados com os interesses dos Estados -. Esta complexidade dificulta a aplicação de disposições legais eficazes em caso de danos em infra-estruturas críticas subaquáticas (Conte de los Ríos, 2023, p. 32).

O regime jurídico aplicável às infra-estruturas submarinas baseia-se em instrumentos internacionais, entre os quais se destacam a Convenção para a Proteção dos Cabos Telegráficos Submarinos, de 1884, e a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), de 1982. Esta última estabelece que todos os Estados têm o direito de instalar cabos e condutas submarinas na plataforma continental, em conformidade com a legislação nacional do Estado costeiro em causa (Arjona Hernández, 2023, p. 48). De igual modo, a CNUDM delimita diferentes espaços marítimos - águas territoriais, Zonas Económicas Exclusivas (ZEE) e alto mar - atribuindo soberania plena nas primeiras, direitos limitados nas ZEE e um quadro regulamentar menos bem definido nas águas internacionais, onde a atividade militar de outros Estados não pode ser legalmente restringida (McNamara, 2024).

Importa referir que, entre os desafios emergentes para o direito marítimo internacional, se encontram os veículos submarinos não tripulados (UUV) e os sistemas marítimos não tripulados (MUS), cujo estatuto jurídico permanece indefinido. A ausência de um quadro regulamentar específico para a sua operação internacional complica a sua integração nos regimes actuais, nomeadamente no que diz respeito à UNCLOS (Conte de los Ríos, 2023, p. 32). Neste contexto, a importância crescente das infra-estruturas subaquáticas críticas torna indispensável avançar para um quadro jurídico internacional eficaz que garanta a sua proteção (García Pérez, 2023, p. 50).

Dada a importância destas infraestruturas e a sua complexa legislação, Michael McNamara (2024) explica que, à medida que as tensões geopolíticas entre o Ocidente e os seus concorrentes aumentam, estas infraestruturas são um alvo, pois a interferência híbrida é uma ferramenta útil no seu objetivo de desafiar os interesses das democracias euro-atlânticas. Estas enfrentam atualmente a sua principal ameaça nas acções híbridas da Rússia (Monaghan et al., 2023, p. 2), particularmente no Mar Báltico, onde tem

reforçado a sua presença investindo em capacidades submarinas, consideradas o seu principal trunfo (Gresh, 2023, pp. 3-4).

Tendo em conta o contexto complexo e a situação do Mar Báltico, peritos como Conte de los Ríos (2025), Njall Trausti Fridbertsson (2023) e Monaghan et al (2023) concordam com uma série de elementos-chave para definir uma estratégia de proteção eficaz. Reconhecendo que é essencial reforçar as capacidades de deteção, dissuasão-prevenção, adaptação e resposta, os elementos a destacar são: (1) o aumento da presença ou da vigilância, (2) a colaboração entre os intervenientes, (3) a coordenação com o sector privado, (4) a tecnologia avançada, (5) os quadros regulamentares, (6) as medidas de resposta e (7) a renovação das estratégias marítimas.

2.3. SITUAÇÃO DAS INFRAESTRUTURAS SUBAQUÁTICAS CRÍTICAS NO MAR BÁLTICO DESDE O INÍCIO DA INVASÃO RUSSA EM GRANDE ESCALA DA UCRÂNIA EM 2022

Em 26 de setembro de 2022, a Autoridade Marítima Dinamarquesa comunicou várias fugas de metano causadas por uma série de explosões submarinas ao largo da ilha dinamarquesa de Bornholm que danificaram gravemente o gasoduto Nord Stream (ver Figura 4), cortando o fornecimento de gás russo ao mercado europeu através do gasoduto Nord Stream (Energistyrelsen, 2022).

Figura 4

Mapa dos gasodutos Nord Stream 1 e Nord Stream 2 junto às fugas de metano detetadas em setembro de 2022.



Fonte: Agência Espacial Europeia (2022).

Independentemente do autor desconhecido da aparente sabotagem, os especialistas concordam que este foi um ponto de viragem para os Aliados considerarem esforços para melhorar a sua capacidade de defesa contra táticas híbridas no domínio dos submarinos (Monaghan, 2022) (Fridbertsson, 2023) (Conte de los Ríos, 2025).

Um caso semelhante foi registado em outubro de 2023 com o incidente no gasoduto Balticconnector. Esta infraestrutura, juntamente com o terminal de gás natural liquefeito (GNL) de Inkoo, salvaguarda a segurança do aprovisionamento e a independência energética dos países da região (ver figura 5).

Figura 5

Mapa da rede de transporte de gás na Finlândia e nos Estados Bálticos.



Fonte: Gasgrid (n.d.)

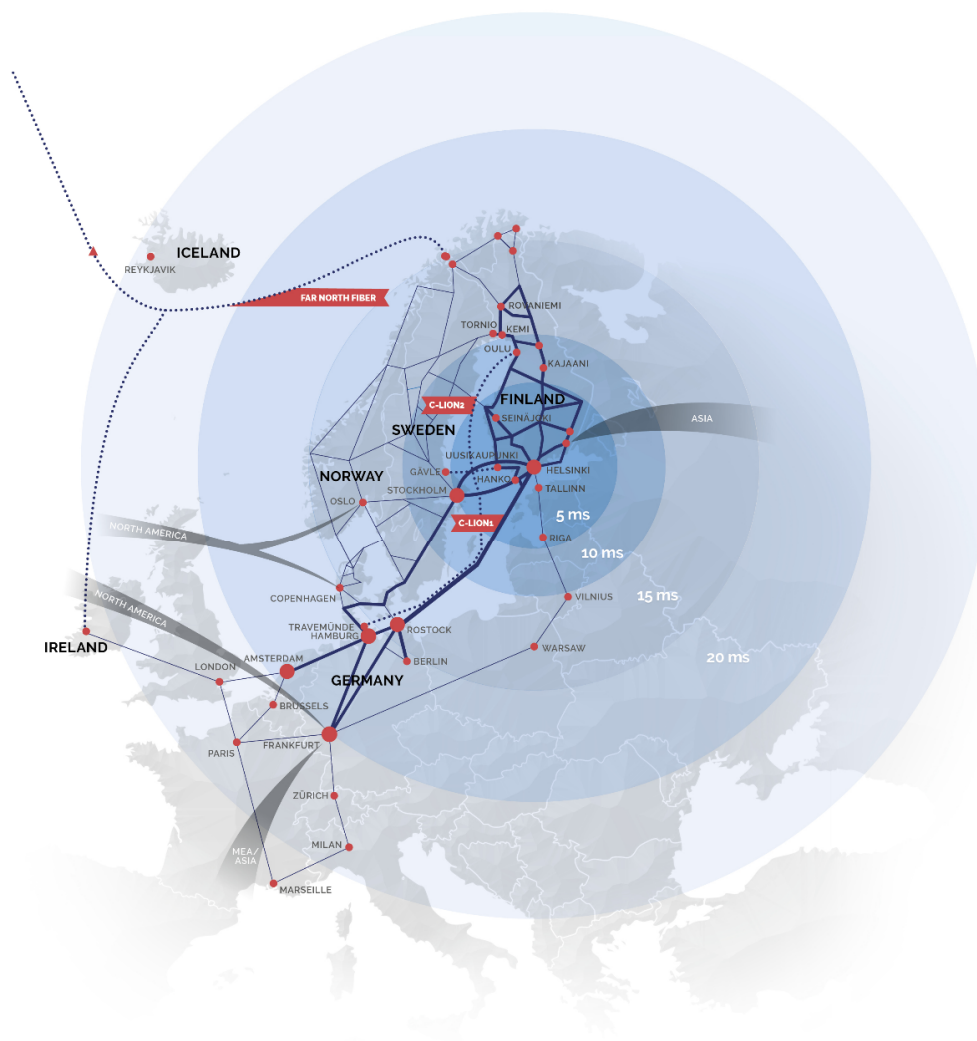
De acordo com os dados fornecidos pelo Serviço Nacional de Investigação finlandês, os danos no oleoduto foram provavelmente causados pelo navio Newnew Polar Bear da companhia de navegação chinesa, que prosseguiu a sua viagem para águas russas escoltado por um navio quebra-gelo do Estado da Eurásia (Polícia da Finlândia, 2023a). Além disso, o Sevmorput, um cargueiro russo de propulsão nuclear, foi também detectado na zona durante o incidente (Polícia da Finlândia, 2023b).

O alegado envolvimento da Rússia neste ataque poderá ter como objetivo desestabilizar o abastecimento energético destes países, que estavam fortemente dependentes do gás russo até este ter sido proibido como resposta à invasão da Ucrânia (Lietuvos Respublikos Energetikos Ministerija, 2022) (Latvijas Vēstnesis, 2022) (Ministério dos Negócios Estrangeiros da República da Estónia, 2022) (Ministério dos Assuntos Económicos e do Emprego da Finlândia, 2024). Já em 2014, nas tentativas dos Estados Bálticos de acelerar a sua desconexão do fornecimento russo através da sincronização das suas redes eléctricas com o apoio da União Europeia (UE), a Lituânia relatou casos de interferência de navios militares russos na instalação do NordBalt, um cabo eléctrico submarino que liga o país à Suécia (McNamara, 2024).

Em novembro de 2024, o cabo submarino C-Lion1, propriedade da empresa finlandesa Cinia, foi aparentemente danificado de forma deliberada. Como este cabo é essencial para a comunicação direta entre a Finlândia e a Alemanha (ver Figura 6), os danos provocaram a interrupção das telecomunicações entre os dois Estados. A gravidade do assunto foi tal que os Ministros dos Negócios Estrangeiros destes países afirmaram, numa declaração conjunta, que as suspeitas de um ataque intencional eram elevadas, referindo que "a segurança europeia não está apenas ameaçada pela guerra de agressão da Rússia contra a Ucrânia, mas também pela guerra híbrida de actores maliciosos" e apelando ao reforço da defesa deste tipo de infra-estruturas na região (Ministério dos Negócios Estrangeiros da Finlândia, 2024).

Figura 6

Mapa da conectividade entre os Estados nórdicos e a Europa Central através dos cabos submarinos C-Lion1 e C-Lion2.



Fonte: Cinia (n.d.)

Simultaneamente, o cabo de telecomunicações BCS East-West Interlink, que liga a Lituânia à Suécia, foi danificado em resultado de "mais do que um simples acidente", como disse Andrius Šemeškevičius, Diretor de Tecnologia da empresa Telia Lietuva, à emissora nacional lituana LRT TV (2024).

As investigações levadas a cabo pelos países envolvidos em ambos os incidentes centraram-se no navio chinês Yi Peng 3, que tinha partido anteriormente do porto russo de Ust-Luga. Não sendo possível abordar o navio, as forças navais dinamarquesas mantiveram-se atentas à sua situação assim que entrou no estreito de Kattegat, como confirmado nas suas redes sociais (Forsvaret, 2024). Com base nas declarações de Šemeškevičius à LRT TV (2024), a probabilidade de sabotagem é bastante elevada, uma vez que os cabos de ambos os incidentes se cruzam (ver Figura 7).

Figura 7

Mapa dos cabos submarinos danificados no Mar Báltico em novembro de 2024 e localização do navio Yi Peng 3.

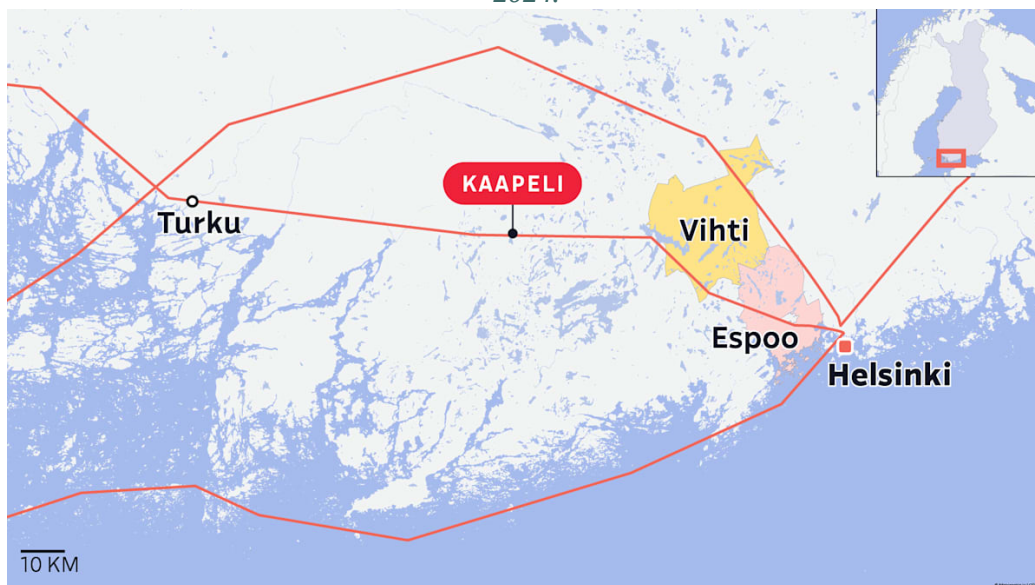


Fonte: Reuters (2024).

Um mês mais tarde, em 3 de dezembro de 2024, a empresa finlandesa GlobalConnect informou que os seus cabos de telecomunicações que ligavam o país à Suécia tinham sido danificados em dois pontos distintos entre as zonas de Vithi e Espoo (ver figura 8), como confirmou o diretor de comunicação da empresa, Niklas Ekström, à emissora pública finlandesa Yle (2024a). No entanto, a polícia finlandesa declarou num comunicado que não havia indícios de sabotagem, mas sim de um acidente devido a danos causados durante as escavações (Polícia da Finlândia, 2025a).

Figura 8

Mapa do cabo submarino da empresa finlandesa GlobalConnect danificado em dezembro de 2024.



Fonte: Yle (2024b).

Em 25 de dezembro de 2024, o operador finlandês Fingrid comunicou que o cabo submarino Estlink 2 da rede eléctrica que liga a Finlândia à Estónia estava danificado (ver Figura 9). A Finlândia iniciou uma investigação de sabotagem e apreendeu o navio-tanque russo "Ghost Fleet" Eagle S, que se encontrava na zona a transportar petróleo russo e que, aparentemente, causou os danos ao arrastar a âncora (Police of Finland, 2025b). Este acontecimento levou a NATO a anunciar, no final de dezembro, a intenção de reforçar a sua presença militar no Mar Báltico para prevenir futuros incidentes e fazer face a eventuais novas ameaças a estas infra-estruturas (NATO, 2024a).

Figura 9

Mapa da conectividade entre a Finlândia e a Estónia através dos cabos submarinos Estlink 1 e Estlink 2.

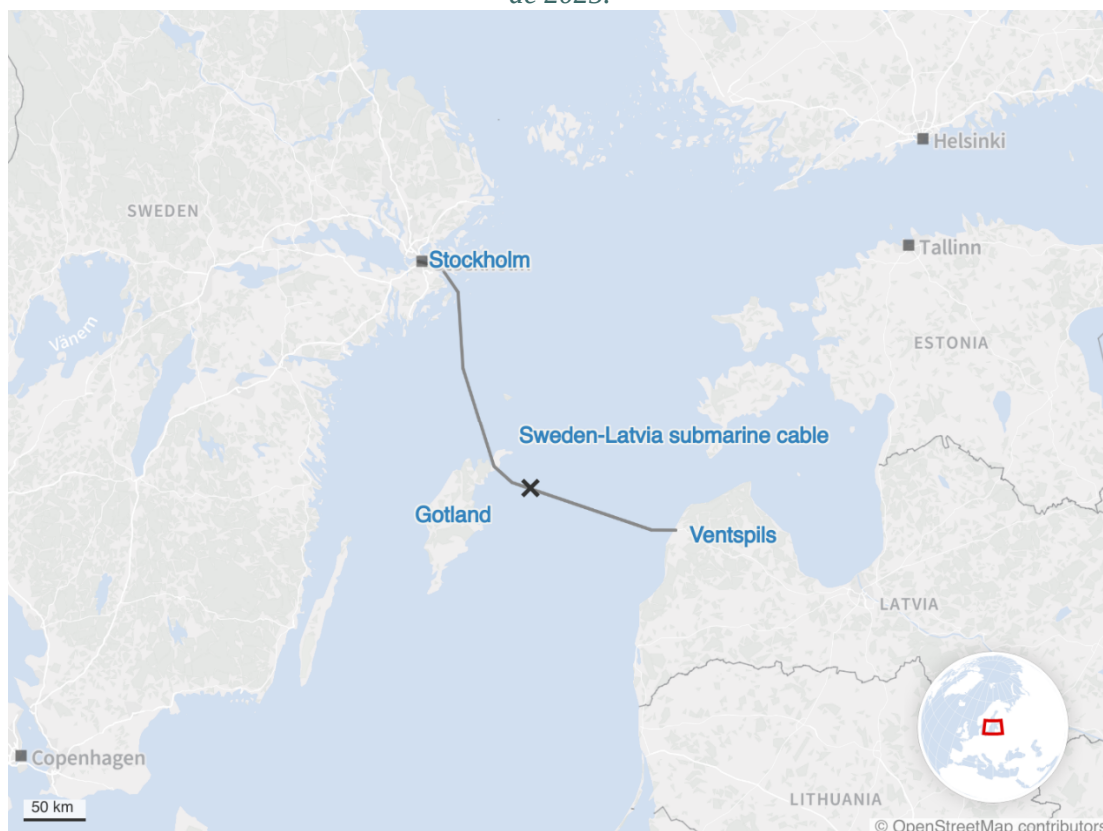


Fonte: Fingrid (n.d.).

Em 26 de janeiro de 2025, foram detectados danos num cabo de comunicações entre a Suécia e a Letónia (ver Figura 10), tal como comunicado pela empresa responsável, o Centro Estatal de Rádio e Televisão da Letónia (2025). Embora o país nórdico tenha aberto um inquérito preliminar por sabotagem e apreendido o cargueiro búlgaro Vezhen, o Ministério Público sueco acabou por determinar que a rutura do cabo entre os dois países não resultou de um ataque deliberado, mas de um acidente (Swedish Prosecution Authority, 2025). Do mesmo modo, a pedido das autoridades letãs, a Noruega apreendeu o Silver Dania, de tripulação russa, que navegava entre São Petersburgo e Murmansk (Politiet, 2025).

Figura 10

Mapa do cabo submarino no Mar Báltico que liga a Letónia e a Suécia danificado em janeiro de 2025.



Fonte: Reuters (2025).

Em fevereiro de 2025, um outro cabo submarino que liga a Finlândia à Alemanha foi danificado na ZEE sueca, perto da ilha sueca de Gotland. Embora a Finlândia já tenha iniciado uma investigação sobre os danos causados ao cabo pertencente a uma das suas empresas (Polícia da Finlândia, 2025c), na Suécia fala-se de uma possível sabotagem. Patrik Johansson, chefe do Departamento de Água e Saneamento da região afetada de Gotland, confirmou, após o primeiro exame do local, que a principal causa foi a influência humana (Região de Gotland, 2025).

Simultaneamente, a empresa finlandesa Cinia (2025) voltou a registar perturbações no funcionamento do cabo submarino C-Lion1. Embora a investigação ainda esteja em curso, o meio de comunicação social alemão Kieler Nachrichten (2025) noticiou que as autoridades alemãs investigaram o cargueiro Arne, um navio suspeito de

fazer parte da "Frota Fantasma Russa", que navegava na zona sob o pavilhão de Antígua e Barbuda e se dirigia de São Petersburgo para Sevilha sem uma das suas âncoras, levantando suspeitas de uma aparente sabotagem orquestrada pelo Kremlin.

Estes incidentes demonstram que as infra-estruturas submarinas críticas na zona são vulneráveis a ataques. Já em 2017, o Comandante da Força de Submarinos da NATO, Andrew Lennon, confirmou a existência de "atividade submarina russa nas proximidades de cabos submarinos" a níveis anteriormente desconhecidos, destacando o interesse estratégico da Rússia nas infraestruturas submarinas da NATO (Birnbaum, 2017). Como observam Monaghan et al. (2023, p. 1), estes potenciais ataques "visam perturbar a coesão transatlântica e a atividade económica, minar o apoio ocidental à Ucrânia e moldar possíveis operações militares futuras". A situação desde o início da guerra tornou, portanto, a segurança nesta área uma prioridade para a NATO.

3. A NATO E A PROTECÇÃO DAS INFRA-ESTRUTURAS SUBMARINAS CRÍTICAS

De um modo geral, a proteção das infra-estruturas submarinas críticas para a NATO está enquadrada em vários artigos do seu tratado fundador. Especificamente, o artigo 2.º sobre a colaboração económica, o artigo 3.º sobre a resiliência e o artigo 5.º sobre a defesa colectiva do Tratado do Atlântico Norte (1949). No que respeita a este último, o Novo Conceito Estratégico da NATO (2022) menciona as ameaças híbridas às infra-estruturas críticas, reafirmando a sua inclusão no quadro do artigo supracitado e salientando o compromisso de cooperação internacional para a sua proteção.

A crescente preocupação com a proteção destas infra-estruturas fez da sua segurança um objetivo particularmente importante para a NATO. Dada a sua importância para o funcionamento da sociedade, ameaças como o controlo adquirido por empresas chinesas sobre algumas destas infraestruturas e a crescente atividade russa nas suas proximidades fizeram com que a Aliança Atlântica considerasse o estado das suas infraestruturas críticas em 2020 (García Pérez, 2023, p. 3).

Relativamente a esta última, o então Secretário-Geral da NATO, Jens Stoltenberg (2020), salientou a importância das infra-estruturas submarinas críticas nos esforços da Aliança para reforçar a sua resiliência:

Penso que é importante abordar esta questão, porque é importante compreender que a maioria destes cabos são propriedade privada e a sua localização é do conhecimento público. E isso torna-os potencialmente vulneráveis. Por isso, temos de monitorizar as potenciais vulnerabilidades. Essa é, em parte, a razão pela qual elaborámos este relatório. Dispomos de ferramentas para os proteger e para monitorizar as ameaças. E também criámos um novo Comando Atlântico em Norfolk, um novo comando da NATO em Norfolk. E uma das tarefas deste novo Comando do Atlântico Norte é também estudar a forma de proteger, de monitorizar as ameaças contra as infra-estruturas submarinas. Por exemplo, a Internet depende destes cabos, o que realça a importância dos cabos submarinos. Uma das principais questões abordadas na reunião de hoje foi a resiliência, que se prende com as infra-estruturas civis, os serviços de saúde e as telecomunicações. Mas, claro, como parte do nosso esforço para reforçar a resiliência, os cabos

submarinos e as infra-estruturas submarinas são uma parte importante desse esforço.

No entanto, as principais medidas para proteger estas infra-estruturas foram adotadas após o início da guerra em grande escala na Ucrânia, em 2022. Até então, esta questão fazia parte do trabalho de instituições limitadas, principalmente ligadas ao domínio marítimo ou à luta contra as ameaças híbridas, duas das quais são particularmente dignas de nota.

Por um lado, o *Compromisso de Resiliência Reforçado*, criado em 2021 por decisão dos Chefes de Estado e de Governo da NATO, que reconhece o compromisso da Aliança em intensificar os esforços para garantir a resiliência das suas infraestruturas críticas (NATO, 2021). Por outro lado, o *Comité de Resiliência da NATO*, órgão responsável pela direção político-estratégica, orientação, planeamento e coordenação geral das atividades de resiliência na Aliança Atlântica (NATO, 2022) (ver Quadro 1).

Quadro 1

Instituições da NATO em que a proteção das infra-estruturas críticas foi enquadrada antes da guerra em grande escala na Ucrânia em 2022.

Instituições de referência	
2006	<i>Centro de Navegação da NATO (NSC)</i>
2007	<i>Centro de Excelência de Cooperação Civil-Militar (CCOE)</i>
2008	<i>Centro de Excelência Cooperativo de Ciberdefesa (CCD COE)</i>
	<i>Comando Marítimo Aliado da NATO (MARCOM)</i>
2012	<i>Centro de Excelência Multinacional para a Proteção do Transporte Marítimo (MARSEC COE)</i>
2014	<i>Centro de Excelência em Comunicação Estratégica</i>
2018	<i>Equipas de apoio contra as ameaças híbridas</i>
2021	<i>Compromisso de Resiliência Reforçada</i>
2022	<i>Comité de Resiliência da NATO</i>

Fonte: Elaboração própria com base nas informações fornecidas pela NATO nos seus sítios Web.

Em resposta à aparente sabotagem do Nord Stream no final de 2022, a NATO criou a *Célula de Coordenação de Infraestruturas Críticas Submarinas* (NATO, 2023a) em fevereiro de 2023. Um mês antes da adoção desta medida, em 11 de janeiro de 2023, foi anunciada a criação de um grupo de trabalho NATO-UE sobre a resiliência das infraestruturas críticas no âmbito do atual Diálogo Estruturado NATO-UE sobre a Resiliência, no qual se insere (Comissão Europeia e NATO, 2023, p. 2).

No seu relatório publicado em junho de 2023, ambas as partes apontam para a existência de uma variedade de ameaças a enfrentar, que vão desde possíveis ataques terroristas a catástrofes naturais. No entanto, salientam diretamente que, desde a agressão russa na Ucrânia, estas infra-estruturas se tornaram um bem vulnerável cuja proteção deve ser uma prioridade (Comissão Europeia e NATO, 2023, p. 4).

Outro exemplo dos efeitos do incidente do Nord Stream como ponto de viragem para o reforço dos esforços ocidentais em matéria de resiliência das suas infraestruturas submarinas críticas é a criação do *Centro Marítimo da NATO para a Segurança das Infraestruturas Submarinas Críticas* (NMCSCUI) na Cimeira de Vilnius em 2023:

A ameaça às infra-estruturas submarinas críticas é real e está a desenvolver-se. Estamos empenhados em identificar e atenuar as vulnerabilidades e dependências estratégicas no que respeita às nossas infra-estruturas críticas e em preparar, dissuadir e defender-nos contra a utilização coerciva da energia e de outras táticas híbridas por parte de intervenientes estatais e não estatais. Qualquer ataque deliberado contra as infra-estruturas críticas dos Aliados será objeto de uma resposta unida e determinada; isto aplica-se igualmente às infra-estruturas críticas submarinas. A proteção das infra-estruturas submarinas críticas no território dos Aliados continua a ser uma responsabilidade nacional, bem como um compromisso coletivo. A NATO está pronta a apoiar os Aliados se e quando tal for solicitado. Concordámos em criar o Centro Marítimo da NATO para a Segurança das Infraestruturas Submarinas Críticas no âmbito do Comando Marítimo da NATO (MARCOM). Também concordámos em criar uma rede que reúna a NATO, os Aliados, o sector privado e outros intervenientes relevantes para melhorar a partilha de informações e o intercâmbio de boas práticas (NATO, 2023b).

Em consonância com Stoltenberg (2020) e com o relatório conjunto da Comissão Europeia e da NATO (2023, p. 3), o Comunicado da Cimeira de Vilnius reafirma a preocupação crescente da Aliança com as ameaças às infra-estruturas submarinas críticas. Neste excerto, a NATO reconhece a necessidade de identificar proactivamente as vulnerabilidades, sublinha que tais ameaças podem emanar tanto de actores estatais como não estatais e salienta a importância de uma coordenação eficaz com os actores relevantes, especialmente do sector privado. Também contempla explicitamente a possibilidade de os ataques híbridos contra estas infra-estruturas poderem ser considerados actos que justifiquem a ativação do artigo 5º da defesa colectiva do Tratado do Atlântico Norte.

O NMCSCUI foi assim inaugurado em maio de 2024. A NATO define-o como uma rede e um centro de conhecimento especializado em infra-estruturas submarinas críticas, cuja principal função é apoiar os processos de decisão estratégica, facilitar o destacamento operacional de forças e coordenar acções conjuntas para garantir a sua proteção. Isto é feito através da integração de esforços entre os Estados membros, parceiros estratégicos e o sector privado (NATO Media Centre, 2024).

No entanto, esta não é a única medida resultante da Cimeira de Vilnius implementada pela NATO para garantir uma melhor resposta às ameaças no domínio marítimo. Em outubro de 2023, foi adoptada a *Digital Ocean Vision*, uma iniciativa que visa melhorar a compreensão do domínio marítimo através de uma maior harmonização das capacidades de vigilância marítima nacionais e aliadas, utilizando uma gama diversificada de meios (NATO, 2023c).

Por outro lado, face aos crescentes desafios a estas infraestruturas, a NATO realizou, a 23 de maio de 2024, a primeira reunião da Rede de Infraestruturas Críticas Submarinas, por decisão dos ministros da defesa, com o objetivo de melhorar a coordenação e a troca de informações. Nesta reunião foram discutidas medidas como o

reforço das patrulhas navais, a promoção da inovação tecnológica e a utilização de capacidades avançadas de deteção e resposta, consolidando o papel central da Aliança nesta área (NATO, 2024b).

Em novembro de 2024, realizou-se em La Spezia, Itália, o Exercício *Bold Machina 24*, coordenado pelo *Comando das Forças de Operações Especiais Aliadas* (SOFCOM) e pelo *Centro de Investigação e Experimentação Marítima* (CMRE), com o objetivo de testar sensores submarinos para proteção de infra-estruturas críticas (NATO Centre for Maritime Research and Experimentation, 2024, p. 2). Estes exercícios reflectem o já referido interesse na integração de tecnologias emergentes, como os sistemas não tripulados, para reforçar a segurança no domínio submarino (Conte de los Ríos, 2025, p. 26).

A este respeito, é também de salientar que a NATO desenvolveu novas ferramentas que permitem aos aliados detetar actividades suspeitas, a fim de se protegerem contra a sabotagem. Estas incluem o uso de inteligência artificial, como exemplificado pelo *Mainsail*, uma ferramenta de software desenvolvida pelo CEMR que detecta embarcações que se comportam de forma suspeita com a intenção de recolher informações e danificar infra-estruturas submarinas (NATO Multimedia, 2025).

No que concerne à proteção específica das infraestruturas submarinas do Mar Báltico, a NATO tem promovido a inovação tecnológica necessária à deteção eficaz de qualquer atividade suspeita para complementar o trabalho das suas patrulhas na região. Estas medidas têm sido progressivamente intensificadas como consequência direta da aparente sabotagem do Nord Stream, como a própria Aliança reconhece (NATO, 2023d).

Em fevereiro de 2025, a NATO realizou uma demonstração de veículos de superfície não tripulados (USV) no Mar Báltico, a fim de promover a sua integração operacional em tarefas de vigilância marítima. Esta iniciativa enquadra-se nos esforços da Aliança para incorporar tecnologias emergentes e disruptivas - como os sistemas autónomos e a inteligência artificial - destinadas a otimizar o conhecimento situacional e a reforçar a proteção de infraestruturas submarinas críticas, em particular ao longo das linhas de comunicação marítimas (NATO Allied Maritime Command, 2025b). Além disso, no âmbito do Comité de Resiliência, a NATO apresentou o seu primeiro *Currículo de Referência de Resiliência* em 2025, com o objetivo de reforçar as capacidades aliadas contra ameaças, incluindo as que visam infraestruturas críticas (NATO, 2025a).

Paralelamente, a cooperação com a União Europeia tem vindo a ganhar importância através de iniciativas como a *EU Hybrid Toolbox*, a *Hybrid Fusion Cell* e as *Hybrid Rapid Response Teams*, destinadas a promover sinergias e a reforçar a coordenação anti-híbrida com a NATO (Serviço Europeu para a Ação Externa, 2022, p. 34). Esta convergência de iniciativas entre as entidades supracitadas demonstra a importância do desenvolvimento de capacidades defensivas robustas, sendo a sua implementação coordenada, juntamente com a integração efectiva de novas tecnologias e capacidades operacionais, essencial para garantir o sucesso da proteção das infra-estruturas submarinas europeias, especialmente tendo em conta a rápida evolução das ameaças que afectam esta área (Conte de los Ríos, 2025, p. 33).

Por último, importa referir que a NATO considera o reforço da cooperação com o sector privado como uma dimensão fundamental para melhorar a sua capacidade de resposta às ameaças às infra-estruturas submarinas críticas. Esta cooperação justifica-se, por um lado, pelo facto de uma parte significativa dessas infraestruturas ser detida ou operada por privados e, por outro lado, pelo potencial do setor privado para fornecer soluções tecnológicas essenciais num ambiente operacional cada vez mais complexo (Fridbertsson, 2023, p. 11).

4. OPERAÇÃO SENTINELA DO BÁLTICO

Em 14 de janeiro de 2025, a NATO realizou uma Cimeira dos Aliados do Mar Báltico para abordar as ameaças crescentes às infra-estruturas submarinas críticas da região. Como resultado, o Secretário-Geral da Aliança Atlântica e os participantes emitiram a *Declaração Conjunta da Cimeira dos Aliados da NATO do Mar Báltico* (2025), anunciando o lançamento de uma iniciativa militar destinada a reforçar a proteção destas infra-estruturas: a Operação *Baltic Sentry*.

Citando a profunda preocupação com o aumento de acções que ameaçam o funcionamento de infra-estruturas submarinas críticas, a Aliança assinalou a sua disponibilidade para "dissuadir, detetar e contrariar qualquer tentativa de sabotagem" e para responder a qualquer ataque "com uma resposta firme e decisiva" (Tasavallan Presidentti, 2025). Isto acontece numa altura em que a NATO reconhece a necessidade de modernizar as suas capacidades para reforçar a sua dissuasão e defesa, a fim de enfrentar e contrariar a evolução das ameaças à segurança (Tasavallan Presidentti, 2025).

O MARCOM, sob a direção do *Comando das Forças Conjuntas* de Brunssum (JFCBS), é reconhecido como tendo um papel fundamental na coordenação das operações no âmbito do que define como uma "atividade de vigilância multi-domínio destinada a aumentar o conhecimento da situação marítima no Mar Báltico para dissuadir e defender contra ataques a infra-estruturas submarinas críticas" (NATO Allied Maritime Command, 2025a). Para esse efeito, a Operação *Baltic Sentry* inclui o destacamento de meios marítimos, aéreos e terrestres adicionais pelos aliados para reforçar a vigilância e a dissuasão.

Através da realização de patrulhas regulares e exercícios conjuntos, a NATO procura manter uma presença constante no Mar Báltico, que é continuamente monitorizado por navios de guerra, submarinos, aeronaves e pelo apoio de tecnologia avançada de vigilância marítima. Por exemplo, os navios do *Standing NATO Maritime Group 1* (SNMG1) e do *Standing NATO Mine Countermeasures Group 1* (SNMCMG1) participarão no *Baltic Sentry* juntamente com outros navios de patrulha marítima aliados, enquanto a NATO continuará a investir em tecnologia militar de ponta para detetar e minimizar as ameaças, como a inteligência artificial, sensores avançados e sistemas de sonar especializados (MARCOM, 2025).

Isto para além da inclusão de dois actores-chave no seio da Aliança. Por um lado, a recém-inaugurada *Força de Intervenção do Comandante* (CTF) no próprio Mar Báltico, sediada na cidade portuária de Rostock. Para além de coordenar os navios aliados no Báltico, a CTF trabalha para construir uma visão regional unificada para as infra-estruturas críticas no Mar Báltico, a fim de apoiar os esforços de proteção estratégica da NATO (Tasavallan Presidentti, 2025). Por outro lado, o já referido NMCSUI centrará

os seus esforços na proteção e segurança dos activos vitais dos submarinos (Tasavallan Presidentti, 2025).

Para atingir estes objectivos, a NATO considera essencial não só trabalhar no seio da própria Aliança, mas também colaborar e cooperar com outros actores, desde a UE ao sector privado. Enquanto no primeiro caso a cooperação se centrará no reforço dos mecanismos existentes, no caso do sector privado a NATO salienta a importância de cooperar com os operadores de infra-estruturas e empresas de tecnologia de ponta no desenvolvimento das diferentes medidas de resposta necessárias para aumentar a resiliência (Tasavallan Presidentti, 2025).

A Aliança Atlântica prevê ainda a adoção de novas medidas, em conformidade com o direito internacional, destinadas tanto à prevenção como à resposta a ameaças ou actos irresponsáveis contra infra-estruturas submarinas críticas na região (Tasavallan Presidentti, 2025). No âmbito do lançamento da Operação *Baltic Sentry*, o atual Secretário-Geral da NATO, Mark Rutte, sublinhou a necessidade de uma aplicação rigorosa do quadro jurídico existente, alertando para o facto de qualquer ameaça potencial contra estas infra-estruturas poder conduzir a medidas coercivas como o apresamento, a apreensão ou a detenção de navios. Neste contexto, apontou a resposta da Finlândia aos incidentes como um exemplo notável de ação (NATO, 2025b).

A aplicação destas medidas é justificada pela constante referência à existência de ameaças. Relativamente a esta última, é mencionada uma ameaça em particular, a chamada "Frota Fantasma Russa". Esta é definida como uma ameaça significativa para a segurança marítima e ambiental, tanto na região do Mar Báltico como a nível mundial, uma vez que compromete a integridade das infra-estruturas submarinas, aumenta os riscos associados às munções químicas depositadas no fundo do mar e representa uma importante fonte de financiamento da guerra ilegal de agressão da Rússia contra a Ucrânia (Tasavallan Presidentti, 2025).

Do mesmo modo, reconhece-se que a ameaça às infra-estruturas submarinas críticas não se limita ao Mar Báltico. Por conseguinte, salienta que a Operação *Baltic Sentry* também representa um ponto de viragem a favor de uma maior cooperação para reforçar a resiliência destas infra-estruturas críticas e, por conseguinte, para reforçar a segurança da NATO. Assim, o lançamento da operação em si é acompanhado pelo anúncio da renovação da estratégia marítima da aliança (Tasavallan Presidentti, 2025).

5. CONCLUSÕES E PROPOSTAS

As infra-estruturas submarinas críticas são vitais para a economia e para o sistema global de comunicações. A sua crescente importância e os constantes avanços tecnológicos nesta área tornaram-nas um alvo prioritário para a defesa, mas também para possíveis ataques. Desta forma, a *Guerra dos Fundos Marinhos* deixou de ser um conceito distante para passar a ser uma ameaça imediata para os Aliados. A estreita ligação entre a segurança destas infra-estruturas e a estabilidade global, nomeadamente em termos económicos e de comunicações, faz com que a sua proteção e a gestão das suas vulnerabilidades sejam hoje uma prioridade de defesa para todos os actores internacionais.

O atual contexto de rivalidade com uma Rússia que anuncia publicamente o seu desejo de desestabilizar a NATO, torna a implementação de estratégias de proteção de infra-estruturas críticas um objetivo extremamente urgente para a defesa da Aliança Atlântica, especialmente na região do Báltico. Como mencionado no documento, o Mar Báltico não é apenas um enclave de competição geopolítica entre a NATO e a Rússia, mas também uma área chave para a segurança de infra-estruturas submarinas críticas que garantem a estabilidade dos Aliados. Unir forças nesta região para reforçar a sua segurança deve, portanto, ser uma prioridade para a NATO, especialmente desde a guerra de 2022 na Ucrânia e a adesão da Suécia e da Finlândia à Aliança.

Isto permite-nos tirar a principal conclusão ligada ao objetivo específico número um deste estudo. Embora a proteção destas infraestruturas já devesse ser um objetivo da NATO, dada a sua importância para a resiliência da sociedade e a sua extrema vulnerabilidade a um vasto leque de ameaças, a atual situação geopolítica torna estas infraestruturas um alvo claro para possíveis ataques. A demonstrá-lo está o aumento de incidentes com cabos submarinos no Mar Báltico desde o início do conflito em 2022, com oito incidentes até à data em que foram danificadas infra-estruturas críticas na região, praticamente todos eles ocorridos na ZEE da Finlândia e da Suécia, países que coincidentemente se candidataram à adesão à NATO nesse mesmo ano, apesar da feroz oposição do Kremlin (ver Quadro 2).

Quadro 2

Incidentes nas infra-estruturas subaquáticas críticas do mar Báltico desde 2022.

	Infra-estruturas	Local do incidente	Países afetados	Causas
Nord Stream	Conduta submarina	ZEEs sueca e dinamarquesa	União Europeia	Altos indícios de sabotagem
Conector do Báltico	Conduta submarina	ZEE finlandesa	Finlândia e Estónia	Altos indícios de sabotagem
C-Lion 1	Cabo de telecomunicações	ZEE sueca	Finlândia e Alemanha	Altos indícios de sabotagem
BCS Interligação Este-Oeste	Cabo de telecomunicações	ZEE sueca	Lituânia e Suécia	Altos indícios de sabotagem
GlobalConnect	Cabos de telecomunicações	ZEE finlandesa	Finlândia e Suécia	Acidente
Estlink 2	Rede eléctrica	ZEE sueca	Finlândia e Estónia	Altos indícios de sabotagem
Centro Estatal de Rádio e Televisão da Letónia	Cabo de telecomunicações	ZEE sueca	Suécia e Letónia	Acidente
Gotlândia	Cabo marítimo propriedade de uma empresa finlandesa	ZEE sueca	Finlândia e Alemanha	Altos indícios de sabotagem

Fonte: Elaboração própria

No que diz respeito ao segundo objetivo específico deste estudo sobre o quadro geral de ação da NATO para a proteção das infra-estruturas submarinas críticas, há várias conclusões a retirar. Apesar do desgaste do desempenho militar russo na guerra da Ucrânia e dos graves reveses sofridos no domínio naval, as táticas híbridas russas continuam a ser a ameaça mais premente às infra-estruturas europeias no Mar Báltico. A NATO está a posicionar-se como um ator central na prevenção de ataques contra essas infra-estruturas, intensificando os seus esforços com medidas progressivas a partir de 2022, na sequência da invasão da Ucrânia e dos incidentes subsequentes.

Enquanto esta questão fazia parte do trabalho de instituições maioritariamente ligadas ao mar, desde a aparente sabotagem do Nord Stream - no meio de tensões com Moscovo - a NATO adoptou quase uma dezena de medidas. Entre elas, a criação da *Célula de Coordenação das Infra-estruturas Críticas Submarinas* ou do *Centro Marítimo da NATO para a Segurança das Infra-estruturas Críticas Submarinas*, a iniciativa *Digital Ocean Vision*, exercícios militares como o *Bold Machina 24*, a inovação tecnológica necessária para tirar partido da inteligência artificial, como o *Mainsail*, e a adoção de iniciativas complementares com terceiros actores, como a UE.

A Operação *Baltic Sentry* é a principal resposta da NATO ao desafio de proteger as infra-estruturas submarinas críticas no Mar Báltico e reforçar a segurança na região. De acordo com o objetivo principal do estudo centrado na análise desta operação, verifica-se que as medidas implementadas no seu âmbito estão orientadas para o reforço das capacidades de deteção, dissuasão-prevenção, adaptação e resposta, estando assim de acordo com os principais critérios propostos pela literatura especializada para a adoção de uma estratégia eficaz (ver Tabela 3).

Quadro 3

Implementação dos elementos necessários para uma estratégia eficaz de proteção das infra-estruturas submarinas críticas no âmbito da Operação Baltic Sentry da NATO.

Operação Sentinela do Báltico da NATO	
Aumento da presença ou da vigilância	✓
Colaboração com actores internacionais	✓
Coordenação com o sector privado	✓
Utilização de tecnologias avançadas	✓
Desenvolvimento de quadros regulamentares	✓
Renovação da estratégia marítima	✓
Aplicação de medidas de resposta	✓

Fonte: Elaboração própria com base em Conte de los Ríos (2025), Monaghan et al. (2023), Fridbertsson (2023) e informações fornecidas pela NATO.

Em suma, a Operação *Baltic Sentry* demonstra que as infraestruturas críticas submarinas são atualmente identificadas pela NATO como uma vulnerabilidade estratégica cuja proteção é essencial para garantir a resiliência e a segurança não só da Aliança, mas também para o dia a dia da sociedade. Uma lição que encontra um ponto de viragem nos diferentes episódios ocorridos no âmbito da guerra na Ucrânia desde 2022, sendo de destacar o aparente ataque ao Nord Stream no final do mesmo ano, como demonstra quer o enquadramento cronológico das medidas adotadas pela NATO neste setor, quer a própria Aliança ao justificar as mesmas.

Assim, respondendo à questão geral da investigação, a hipótese geral do estudo é que a Operação *Baltic Sentry* reforça a proteção das infra-estruturas submarinas críticas no Mar Báltico e a presença da Aliança no Mar Báltico, ajustando-se assim ao novo contexto de ameaça.

REFERÊNCIAS BIBLIOGRÁFICAS

- Arjona Hernández, N. (2023). A proteção dos cabos submarinos de telecomunicações: Soberanias digitais e segurança da rede de cabos submarinos. *International Journal Of Policy Thinking*, 18(18), pp. 41-67. <https://doi.org/10.46661/revintpensampolit.8753>
- Comissão para a Proteção do Meio Marinho do Báltico (2024). *Serviço de mapas e dados da HELCOM*. <https://maps.helcom.fi/website/mapservice/>
- Comissão para a Proteção do Meio Marinho do Báltico (2024). *Serviço de mapas e dados da HELCOM*. <https://maps.helcom.fi/website/mapservice/>
- Birnbaum, M. (22 de dezembro de 2017). Os submarinos russos estão a rondar cabos submarinos vitais. Isso está a deixar a NATO nervosa. *The Washington Post*. https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?hpid=hp_hp-top-table-main_russiasubs712pm%3Ahomepage%2Fstory
- Bueger, C., Liebetrau, T., e Franken, J. (2022). *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU [Ameaças à segurança dos cabos e infraestruturas de comunicações submarinas - Consequências para a UE]*. Análise aprofundada do Parlamento Europeu, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)
- Bueger, C., e Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network [Proteger infra-estruturas ocultas: a política de segurança da rede mundial de cabos submarinos de dados]. *Contemporary Security Policy*, 42(3), pp. 391-413. <https://doi.org/10.1080/13523260.2021.1907129>
- Cassetta, M. (2024). Como responder às ameaças emergentes às infra-estruturas subaquáticas críticas na altura da guerra da Rússia contra a Ucrânia. *Istituto Affari Internazionali (IAI), IAI Commentaries 24-31 de junho de 2024*, pp. 1-5. <https://www.iai.it/en/pubblicazioni/c05/how-respond-emerging-threats-critical-underwater-infrastructure>
- Childs, N. (2025). A "Frota Sombra" da Rússia e a evasão às sanções: o que fazer? *Instituto Internacional de Estudos Estratégicos (IISS), janeiro de 2025*, pp. 1-15. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf
- Cinia (20 de fevereiro de 2025). *Perturbação no cabo submarino C-Lion da Cinia*. <https://www.cinia.fi/en/news/disturbance-in-cinia-c-lion-submarine-cable>

- Cinia (n.d.). *Conectividade internacional da Cinia*. <https://www.cinia.fi/hubfs/Cinia%20Theme%202024/Muut%20kuvat/Cinian-kansainvaliset-verkkoyhteydet-kartta.jpg>
- Clark, B. (2015). *The Emerging Era in Undersea Warfare [A Era Emergente da Guerra Submarina]*. Centro de Avaliações Estratégicas e Orçamentais (CSBA), <https://csbaonline.org/research/publications/undersea-warfare>
- Conte de los Ríos, A. (2025). Ameaças à segurança: fundos marinhos e infra-estruturas críticas. *Global Affairs Journal*, (7), pp. 26-35. <https://www.unav.edu/documents/16800098/147587031/amenazas-seguridad.pdf>
- Deni, J. R. (18 de dezembro de 2023). *O Mar Báltico é um lago da NATO?* Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake?lang=en>
- Energistyrelsen (26 de setembro de 2022). *Fuga no North Stream 2 no Mar Báltico*. <https://ens.dk/en/press/leak-north-stream-2-baltic-sea>
- Comissão Europeia e NATO . (2023). *TASK OF FORCE UE-NATO SOBRE A RESILIÊNCIA DAS INFRA-ESTRUTURAS CRÍTICAS. RELATÓRIO DE AVALIAÇÃO FINAL*. https://www.nato.int/cps/en/natohq/news_216631.htm
- Serviço Europeu para a Ação Externa (2022). *UMA BÚSSOLA ESTRATÉGICA PARA A SEGURANÇA E A DEFESA: Por uma União Europeia que proteja os seus cidadãos, valores e interesses e contribua para a paz e a segurança internacionais*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
- Fingrid (n.d.). *EstLink 2 - segunda ligação de corrente contínua de alta tensão entre a Finlândia e a Estónia*. <https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/>
- Fink, A. e Kofman, M. (2020). Estratégia Russa para a Gestão da Escalada: Principais Debates e Actores no Pensamento Militar. *Memorando de Informação do CNA, abril de 2020*, pp. 1-48. https://www.cna.org/cna_files/pdf/DIM-2020-U-026101-Final.pdf
- Foggo, J. (17 de janeiro de 2023). A Quarta Batalha do Atlântico está a decorrer. *Centro de Análise de Política Europeia (CEPA)*, <https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/>
- Foggo, J. e Fritz, A. (2016). The Fourth Battle of the Atlantic. *U.S. Naval Institute*, 142(6), <https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic>
- Forsvaret. [@forsvaretdk] (20 de novembro de 2024). *Relativamente ao navio chinês Yi Peng 3: A Defesa dinamarquesa pode confirmar que estamos presentes na área*

próxima do navio chinês Yi Peng 3. A Defesa dinamarquesa não tem mais comentários. [Post in X].
<https://x.com/forsvaretdk/status/1859195509866381402>

Fridbertsson, N. T. (2023). *Proteção das infra-estruturas marítimas críticas - O papel da tecnologia*. Relatório Geral. 032 STC 23 E. Assembleia Parlamentar da NATO: Comité de Ciência e Tecnologia (STC). <https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc>

García Pérez, R. (2023). Espanha na rede mundial de cabos submarinos. *Instituto Español de Estudios Estratégicos, Documento Marco IEEE 10/2023*, pp. 1-51. <https://www.defensa.gob.es/ceseden/-/espa%C3%B1a-en-la-red-global-de-cables-submarinos>

García Pérez, R. (2024). "La seguridad de los cables submarinos", in Fernando Ibáñez Gómez (Coord.), *Seguridad marítima. Una incertidumbre permanente*, Bosch Editor, Barcelona, pp. 265-298.

Gasgrid (n.d.). *Mapa das transmissões de gás da Finlândia e do Báltico*. https://gasgrid.fi/wp-content/uploads/Gasgrid_maakaasu_lisaversiot_eu_EN-scaled.jpg

Gasum (2023). *A Gasum rescindiu o seu contrato de fornecimento de gás natural por gasoduto com a Gazprom Export*. <https://www.gasum.com/en/news-and-customer-stories/news-and-press-releases/2023/gasum-has-terminated-its-pipeline-natural-gas-supply-contract-with-gazprom-export/#:~:text=The%20parties%20were%20not%20able,details%20of%20the%20contract%20termination>.

Gresh, G. F. (2023). *A nova realidade da segurança marítima da Europa: portos chineses, bases russas e a ascensão da guerra submarina*. Foreign Policy at Brookings, Policy Brief, fevereiro de 2023. <https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/>

Guilfoyle, D., Paige, T. P., e McLaughlin, R. (2022). A ÚLTIMA FRONTEIRA DO CIBERESPAÇO: OS FUNDOS MARINHOS PARA ALÉM DA JURISDIÇÃO NACIONAL E A PROTECÇÃO DOS CABOS SUBMARINOS. *International and Comparative Law Quarterly*, 71(3), pp. 657-696. <https://doi.org/10.1017/S0020589322000227>

Grupo Insikt (2023). *The Escalating Global Risk Environment for Submarine Cables*. Análise de Ameaças do Futuro Registada, <https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables>

Comité Internacional de Proteção dos Cabos (2024). *Relatório do Comité Internacional de Proteção de Cabos Docs: HSSC16-07.10A: Actividades do ICPC que afectam a HSSC*. Organização Hidrográfica Internacional, Tóquio, Japão, 27-31 de maio

- de 2024.
https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf
- Jones, S. G. (2025). Russia's Shadow War Against the West [A Guerra Sombra da Rússia contra o Ocidente]. *Centro de Estudos Estratégicos e Internacionais (CSIS), CSIS Briefs March 2025*, pp. 1-20. <https://www.csis.org/analysis/russias-shadow-war-against-west>
- Kaushal, S. (25 de maio de 2023). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*. Royal United Services Institute (RUSI), maio de 2023. <https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure>
- Kieler Nachrichten (2025). *Verdacht der Sabotage: Ermittler suchen Anker vom russischen Frachter "Arne"* [Suspeita de sabotagem: Investigadores procuram a âncora do cargueiro russo "Arne"]. <https://www.kn-online.de/schleswig-holstein/verdacht-der-sabotage-gegen-russischen-frachter-arne-in-kiel-ermittlungsstand-ORSQRUDZZRGJHC7KSCB4SKJCDM.html>
- Centro Estatal de Rádio e Televisão da Letónia (2025). *Cabo de fibra ótica submarino do LVRTC danificado*. <https://www.lvrtc.lv/en/news/jaunumi/lvrtc-submarine-optical-fiber-cable-damaged/>
- Latvijas Vēstnesis (28 de julho de 2022). *Grozījumi Enerģētikas likumā* [Alterações à lei da energia]. <https://www.vestnesis.lv/op/2022/144.5>
- Lietuvos Respublikos Energetikos Ministerija (20 de maio de 2022). *A partir de domingo, a Lituânia deixará de importar petróleo, gás e eletricidade russos*. <https://enmin.lrv.lt/en/news/no-more-russian-oil-gas-and-electricity-imports-in-lithuania-from-sunday/>
- LRT TV (18 de novembro de 2024). *Cabo submarino entre a Lituânia e a Suécia danificado - Telia*. https://www.lrt.lt/en/news-in-english/19/2416006/undersea-cable-between-lithuania-and-sweden-damaged-telia?srsId=AfmBOoowPquC_SbY0w-dUT2dfxJTzPrj-OPvif6IxXoDTJQuKnQx11fF
- McNamara, E. M. (17 de março de 2016). *Garantir a segurança da região nórdico-báltica*. Notícias da NATO. <https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html>
- McNamara, E. M. (28 de agosto de 2024). *Reforço da resiliência: o papel da NATO no reforço da segurança das infraestruturas submarinas críticas*. *NATO Review: Opinion, Analysis and debate on Security Issues*, <https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html>

Ministério dos Negócios Estrangeiros da Finlândia (18 de novembro de 2024). *Declaração conjunta dos Ministros dos Negócios Estrangeiros da Finlândia e da Alemanha sobre o cabo submarino cortado no Mar Báltico*. https://um.fi/statements/-/asset_publisher/6zHpMjnoIHgl/content/joint-statement-by-the-foreign-ministers-of-finland-and-germany-on-the-severed-undersea-cable-in-the-baltic-sea/35732

Ministério dos Assuntos Económicos e do Emprego da Finlândia (7 de maio de 2024). *Hallituksen esitys laiksi laiksi maakaasun ja nesteytetyn maakaasun maahantuonnin väliaikaisesta kieltämisestä Venäjän federaatiosta ja Valko-Venäjältä* [Proposta de lei do Governo sobre a proibição temporária da importação de gás natural e gás natural liquefeito da Federação Russa e da Bielorrússia]. <https://tem.fi/en/project?tunnus=TEM036:00/2024>

Monaghan, S. (6 de outubro de 2022). Cinco passos que a NATO deve dar após o ataque ao gasoduto Nord Stream. *Centro de Estudos Estratégicos e Internacionais (CSIS)*, <https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack>

Comando Marítimo Aliado da NATO (2025a, 14 de janeiro de 2025). *O Baltic Sentry da NATO intensifica as patrulhas no Mar Báltico para salvaguardar as infraestruturas submarinas críticas*. <https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure>

Comando Marítimo Aliado da NATO (2025b, 20 de fevereiro de 2025). *A NATO efectua uma demonstração de veículos de superfície não tripulados no Mar Báltico*. <https://mc.nato.int/media-centre/news/2025/page228602539>

Centro de Investigação e Experimentação Marítima da NATO (2024). *BOLETIM INFORMATIVO DA NATO STO CMRE*. January-June 2024. [https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20\(002\).pdf](https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20(002).pdf)

Centro de Comunicação Social da NATO (2024, 28 de maio de 2024). *A NATO lança oficialmente o novo Centro Marítimo para a Segurança das Infraestruturas Submarinas Críticas*. <https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui>

Multimédia da NATO (06 de fevereiro de 2025). *Proteção dos cabos submarinos com inteligência artificial*. <https://www.natomultimedia.tv/app/asset/718197>

NATO (2021, 14 de junho de 2021). *Compromisso de Resiliência Reforçada*. https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO (2022, 07 de outubro de 2022). *Comité de Resiliência*. https://www.nato.int/cps/in/natohq/topics_50093.htm

NATO (2023a, 15 de fevereiro de 2023). *A NATO cria uma célula de coordenação das infraestruturas submarinas*.
https://www.nato.int/cps/en/natohq/news_211919.htm

NATO (2023b, 11 de julho de 2023). *Comunicado da Cimeira de Vilnius. Emitido pelos Chefes de Estado e de Governo da NATO que participam na reunião do Conselho do Atlântico Norte em Vilnius, em 11 de julho de 2023*.
https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO (2023c, 12 de outubro de 2023). *Ministros da Defesa da NATO lançam iniciativa para reforçar as capacidades de vigilância marítima*.
https://www.nato.int/cps/ra/natohq/news_219441.htm

NATO (2023d, 19 de outubro de 2023). *A NATO intensifica as patrulhas no Mar Báltico após danos nas infraestruturas submarinas*.
https://www.nato.int/cps/en/natohq/news_219500.htm

NATO (2024a, 30 de dezembro de 2024). *A NATO reforçará a presença militar no mar Báltico*. https://www.nato.int/cps/en/natohq/news_231800.htm

NATO (2024b, 23 de maio de 2024). *A NATO realiza a primeira reunião da Rede de Infraestruturas Submarinas Críticas*.
https://www.nato.int/cps/en/natohq/news_225582.htm

NATO (2025a, 21 de fevereiro de 2025). *A NATO lança o Currículo de Referência da Resiliência*. https://www.nato.int/cps/en/natohq/news_233458.htm

NATO (2025b, 14 de janeiro de 2025). *A NATO lança o "Baltic Sentry" para aumentar a segurança das infra-estruturas críticas*.
https://www.nato.int/cps/en/natohq/news_232122.htm

Polícia da Finlândia (2025b, 2 de março de 2025). *O navio-tanque Eagle S vai passar para águas internacionais sob o controlo da Guarda de Fronteiras*.
<https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control>

Polícia da Finlândia (2023a, 24 de outubro de 2023). *O Serviço Nacional de Investigação esclareceu tecnicamente a causa dos danos no gasoduto*. <https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage>

Polícia da Finlândia (2023b, 17 de outubro de 2023). *O Serviço Nacional de Investigação examina os antecedentes dos navios que navegam na zona de danos do gasoduto*.
<https://poliisi.fi/en/-/national-bureau-of-investigation-examines-background-of-vessels-sailing-in-the-gas-pipeline-damage-area>

Polícia da Finlândia (2025a, 3 de dezembro de 2025). *A polícia não suspeita de qualquer infração penal em nenhum dos incidentes de danos em cabos no sul da Finlândia*.
<https://poliisi.fi/en/-/police-do-not-suspect-any-criminal-offence-in-either-of-the-cable-damage-incidents-in-southern-finland>

Polícia da Finlândia (2025c, 21 de fevereiro de 2025). *O Serviço Nacional de Investigação vai efetuar um inquérito preliminar sobre a suspeita de danos nos cabos no Mar Báltico*. <https://poliisi.fi/en/-/national-bureau-of-investigation-to-conduct-a-preliminary-inquiry-into-suspected-cable-damage-in-baltic-sea>

Politiet (31 de janeiro de 2025). *O navio pode sair de Tromsø*. <https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2025/01/31/troms2/>

Quijarro Santibáñez, L. (2023). Guerra nos fundos marinhos: a guerra submarina no século XXI. *Revista de Marina*, 141(997), pp. 15-22. <https://revistamarina.cl/revista/997>

Região de Gotland (3 de março de 2025). *Misstänkt sabotage* [Suspeita de sabotagem]. <https://gotland.se/bygga-bo-och-miljo/vatten-och-avlopp/dricksvatten/misstankt-sabotage>

República da Estónia Ministério dos Negócios Estrangeiros . (2022). *A Estónia impõe uma proibição das importações e aquisições de gás natural da Rússia*. <https://www.vm.ee/en/news/estonia-imposes-ban-natural-gas-imports-and-purchases-russia>

Reuters (2024). *Cabos de fibra ótica danificados no Mar Báltico*. <https://www.reuters.com/graphics/BALTICSEA-CABLES/zdpxqaaxwvx/chart.png>

Reuters (2025). *Cabo de fibra ótica danificado no Mar Báltico*. <https://www.reuters.com/graphics/BALTIC-SECURITY/xmvjbdamavr/chart.png>

Stoltenberg, J. (22 de outubro de 2020). *Conferência de imprensa online do Secretário-Geral da NATO, Jens Stoltenberg, após o primeiro dia das reuniões dos Ministros da Defesa da NATO*. https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Fórum das Telecomunicações Submarinas (2025). *Perspectivas globais*. Revista SubTel Forum #140. <https://subtelforum.com/subtel-forum-magazine-140-global-outlook/>

Ministério Público sueco (2025). *Procurador revoga decisão sobre navio apreendido*. https://www.aklagare.se/en/media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/?_t_id=ajCngOfkVK4qcLdxSmm4EA%3d%3d&_t_uuid=ajbjBKKEs7uVHPgMJkVsvA&_t_q=baltic&_t_tags=language%3aen%2csiteid%3a764c28f6-3ce5-48e7-a8ec-b8f5f22e4245%2candquerymatch&_t_hit.id=Aklagare_Web_Business_PressReleases_Models_PressReleasePage/_847c0fdb-df1d-4d16-9b4a-0db494be3af4_en&_t_hit.pos=2

Tasavallan Presidentti (14 de janeiro de 2025). *Declaração conjunta da Cimeira dos Aliados da NATO do Mar Báltico*. <https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/>

Agência Espacial Europeia (06 de outubro de 2022). *Mapa do gasoduto Nordstream com o tráfego marítimo*. https://www.esa.int/ESA_Multimedia/Images/2022/10/Nordstream_pipeline_map_with_shipping_traffic

Yle (2024a, 31 de dezembro de 2024). *Polícia: não há suspeita de crime na rutura do cabo entre a Finlândia e a Suécia*. <https://yle.fi/a/74-20128835>

Yle (2024b). *O cabo foi danificado em dois locais distintos entre Espoo e Vihti*. Image: Laura Merikalla / Yle, Mapcreator, OpenStreetMap, GlobalConnect. https://images.cdn.yle.fi/image/upload/c_crop,h_1080,w_1919,x_0,y_0/ar_1.7777777777777777,c_fill,g_faces,h_675,w_1200/dpr_2.0/q_auto:eco/f_auto/fl_lossy/v1733216443/39-1389673674ec7f18a492

REGULAMENTO

Convenção das Nações Unidas sobre o Direito do Mar, Nova Iorque, 30 de abril de 1982.
https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Convenção para a Proteção dos Cabos Telegráficos Submarinos, Paris, 14 de março de 1884.
https://iscpc.org/information/Convention_on_Protection%20of_Cables_1884.pdf

Novo Conceito Estratégico da NATO, Madrid, 29 de junho de 2022.
https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_o_tan.pdf

Tratado do Atlântico Norte, Washington, 4 de abril de 1949.
https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es



Artigo de investigação

O CAPITAL INTELECTUAL NA INSTITUIÇÃO DA GUARDIA CIVIL E A SUA CONTRIBUIÇÃO PARA A ECONOMIA SOCIAL

Tradução para o português com ajuda de IA (DeepL)

Virgínia Belén Subiris Moriel

Estudante de doutoramento na Universidade Rey Juan Carlos.

Programa de Ciências Sociais e Jurídicas. Ramo de atividade

Mestrado em Gestão Internacional de Recursos Humanos

(Gestão Internacional de Recursos Humanos)

virbelsu@gmail.com

ORCID: <https://orcid.org/0009-0000-2569-3710>

Recebido em 31/03/2025

Aceite em 10/06/2025

Publicado em 27/06/2025

Citação recomendada: Subiris, V. (2025). O capital intelectual na instituição da Guardia Civil e a sua contribuição para a economia social. *Revista Logos Guardia Civil*, 3(2), p.p. 257-292.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

O CAPITAL INTELECTUAL DA GUARDA CIVIL E A SUA CONTRIBUIÇÃO PARA A ECONOMIA SOCIAL

Resumo: INTRODUÇÃO. 2. ENQUADRAMENTO TEÓRICO. 2.1. Capital intelectual. 2.2. A Economia Social e o Corpo de Guardia Civil. 3. 3. METODOLOGIA. 4. RESULTADOS E DISCUSSÃO. 5. CONCLUSÕES E PROPOSTAS. 6. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: A segurança é uma questão fundamental para a cooperação entre os países que compõem a União Europeia no atual contexto socioeconómico. Isto implica que as políticas do sector público não devem apenas reforçar as capacidades de defesa, mas também implementar medidas que contribuam para a segurança económica e social. A ligação destes termos: segurança, cooperação, economia pública e social, leva-nos a pensar numa instituição que os tem alinhado na sua estratégia ao longo de mais de 181 anos de existência, a Instituição da Guarda Civil. No entanto, não foram encontradas pesquisas, artigos ou projetos que abordem essa questão no âmbito académico. Este estudo analisa como o capital intelectual (CI) da instituição contribui para a geração de valor socioeconómico através das suas acções solidárias e humanitárias. A metodologia utilizada baseia-se numa análise de conteúdo da informação divulgada sobre o seu CI nos seus relatórios de responsabilidade social e sustentabilidade entre 2014-2023. O modelo Intellectus adaptado ao contexto público foi utilizado para identificar e quantificar os activos intangíveis. Os resultados mostram que o CI da Instituição, através da gestão do conhecimento, da cultura organizacional, das relações externas, do carácter benévolo e do compromisso social, proporciona um valor tangível e intangível que vai para além das suas funções de segurança pública. Esta investigação demonstra a relevância do CI nas instituições públicas e o seu potencial no reforço de uma economia social integrada na Agenda 2030.

Resumen: La seguridad es un tema clave para la cooperación entre los países que conforman la Unión Europea en el entorno socioeconómico actual. Esto implica que las políticas del sector público no sólo fortalezcan las capacidades en defensa, sino que también implementen medidas que contribuyan a la seguridad económica y social. Conectando estos términos: seguridad, cooperación, público y economía social, nos lleva a pensar en una institución que los ha alineado en su estrategia, durante más de 181 años de existencia, la Institución de la Guardia Civil. Sin embargo, no se han encontrado investigación, artículos o proyectos que aborden esta cuestión en el ámbito académico. El presente estudio analiza cómo el capital intelectual (CI) de la institución, contribuye a generar valor económico-social a través de sus acciones solidarias y humanitarias. La metodología utilizada se basa en un análisis de contenido de la información divulgada de su CI en sus memorias de responsabilidad social y de sostenibilidad entre 2014-2023. Se ha empleado el modelo Intellectus adaptado al contexto público, para identificar y cuantificar los activos intangibles. Los resultados evidencian que el CI de la Institución, a través de la gestión del conocimiento, la cultura organizativa, las relaciones externas, el carácter benemérito y el compromiso social aporta valor tangible e intangible que va más allá de sus funciones de seguridad pública. Esta investigación demuestra la relevancia del CI en instituciones públicas y su potencial en el fortalecimiento de una economía social integrada en la Agenda 2030.

Palavras-chave: economia social, capital intelectual, guarda civil, sustentabilidade, valor social.

Palabras clave: economía social, capital intelectual, guardia civil, sostenibilidad, valor social.

ABREVIATURAS

ASGC: Associação de Guardas Cívicas Solidárias.

CEPES: Confederação Empresarial da Economia Social Espanhola.

CE: Capital estrutural.

CH: Capital humano.

QI: Capital Intelectual.

CIC: Centro de Investigação sobre a Sociedade do Conhecimento.

CIS: Centro de Investigação Sociológica.

CR: Capital Relacional.

EUROPOL: Polícia Europeia.

IADE: Instituto de Administração de Empresas.

KBW: Knowledge- Based View (visão baseada no conhecimento).

MITES: Ministério do Trabalho e da Economia Social.

MRSCGC: Relatório de Responsabilidade Social Corporativa da Guardia Civil.

MS: Relatório de Sustentabilidade.

RBV: Resources- Based View (visão baseada em recursos).

RSE: Responsabilidade Social das Empresas.

ODS: Objectivos de Desenvolvimento Sustentável.

OECC: Gabinete Espanhol para as Alterações Climáticas

OCDE: Organização para a Cooperação e Desenvolvimento Económico.

ONG: Organização não governamental.

ONU: Nações Unidas.

NATO: Organização do Atlântico Norte.

UE: União Europeia.

VRIN: Valor, Raridade, Inimitabilidade e Não-Substituibilidade.

1. INTRODUÇÃO

A economia social é um modelo económico centrado no interesse coletivo que coloca as pessoas no centro da sua atividade, dando prioridade à cooperação, à sustentabilidade e à solidariedade em detrimento do lucro individual (Retolaza & Alzola, 2021). O desenvolvimento contínuo das economias e das sociedades exige que se dê prioridade às medidas que melhoram a produtividade em todos os sectores industriais. É particularmente interessante analisar como uma instituição pública como a Guardia Civil, que coloca as pessoas no centro do seu modelo de negócio, integra os princípios da economia social na sua missão de garantir a segurança pública.

Atualmente, a economia social tem sido promovida pelo Comité Económico e Social Europeu, centrando-se na interdependência entre a economia e a sociedade. Em Espanha, o conceito foi amplamente divulgado pela Confederação Empresarial Espanhola da Economia Social (CEPES). Além disso, a lei 5/2011, de 29 de março, no seu Preâmbulo, agrupa os princípios de diferenciação das entidades da economia social, sendo um deles: o enfoque nas pessoas e o objetivo social, como o principal. Neste contexto, as organizações participantes acolhem projetos sociais realizados individualmente, como instituições com outra forma jurídica (Sánchez et al., 2018). Alinhado com o Plano Integral para uma Cultura de Segurança Nacional, uma vez que é desenvolvido de acordo com os Objetivos de Desenvolvimento Sustentável (ODS) estabelecidos pela Agenda 2030. Para evoluir, requer a colaboração ativa de todos os setores que compõem o ecossistema social, desde organizações privadas a públicas, incluindo organizações da sociedade civil, sem esquecer o setor académico (García-Flores & Palma, 2020).

Na sequência do ponto anterior, pode dizer-se que a instituição da Guarda Civil pertencente ao sector público apresenta uma abordagem integrada na economia social através das dimensões ou capitais que constituem o seu capital intelectual (CI). Desde a sua criação, a instituição da Guarda Civil tem baseado as suas acções na segurança, prevenção e proteção dos direitos e liberdades dos cidadãos, mas também no seu cuidado e assistência quando se encontram em situação de vulnerabilidade (capital humano). Neste sentido, fomenta a participação e a articulação interna e externa com diferentes entidades, o que se designa por carácter benévolo (capital estrutural). Este intangível, aliado a outros tangíveis como a estrutura e a diversificação da instituição, não só serve para reforçar alianças que fomentam redes sociais já estabelecidas, como também é utilizado como facilitador de ligações entre comunidades e indivíduos distantes (Burt, 2004) (capital relacional). Não esquecendo que a coesão e a confiança geradas nestas relações facilitam a transmissão de conhecimento, que é um intangível valorizado na economia (Arteaga et al., 2020).

A investigação sobre o CI tem demonstrado a relevância do valor que lhe é atribuído. Garanina et al., (2021), numa revisão estruturada em diferentes países realizada no período (2010-2020), observaram a convergência dos investigadores para concetualizar o conceito de CI como gerador de valor empresarial. Neste artigo, evitaremos entrar na retórica sobre o valor dos intangíveis versus tangíveis, uma vez que, atualmente, a controvérsia da era pós-industrial dos anos 70 ficou para trás. Nessa altura, o valor dos activos incorpóreos de uma empresa começava a ser objeto de debate nos relatórios financeiros. Igualmente esquecidas estão as controvérsias levantadas a seu respeito após o rebentamento da bolha dotcom, a crise financeira global de 2008, quando

as empresas começaram a avaliar os "riscos" e um período de relativa estagnação económica (Hazan et al., 2021).

A academia indica que o paradigma do CI é considerado estabelecido como um sistema para a obtenção de valor empresarial entre os académicos no final de 2010 e, portanto, alcançou consolidação teórica nos dias de hoje. Consequentemente, o objetivo deste estudo é analisar em que medida as ações solidárias e humanitárias da Instituição Guarda Civil geram valor social para os stakeholders, impactando na economia social por meio da gestão dos elementos que compõem o seu CI, pois são fundamentais para o crescimento e desenvolvimento social (Haskel & Weslake, 2018; Stratone, 2023). A nossa decisão baseia-se no preenchimento de uma lacuna encontrada na aplicação de uma abordagem de CI a uma instituição pública enquanto agente ativo na economia social e tradicionalmente estudada através de um prisma operacional e legal. Ao tornar estes princípios visíveis na Instituição Guarda Civil, pretendemos abrir outras linhas de investigação que não têm sido tão exploradas na economia social e nos organismos de aplicação da lei nacionais e internacionais no seu estudo do CI.

Este artigo está estruturado da seguinte forma: na primeira secção, fazemos uma breve revisão e definimos o conceito de Capital Intelectual (CI). Em seguida, na segunda secção, analisamos as sinergias entre a Economia Social e a instituição objeto da nossa investigação e inferimos as nossas hipóteses de investigação. Estas hipóteses são apresentadas na terceira secção, que trata da metodologia utilizada. Em consonância com esta última, a quarta secção apresenta os resultados obtidos com a investigação, terminando com a quinta secção sobre as conclusões retiradas, contributos e limitações.

2. QUADRO TEÓRICO

2.1. CAPITAL INTELECTUAL (CI)

As empresas, a nível micro ou macro, em qualquer sector, devem considerar tanto os seus activos tangíveis como os intangíveis úteis para a criação de valor, o que é frequentemente referido como capital intelectual (Cañibano, et al., 2002; Bueno et al., 2008; Fernández et al., 2022). Este adquire relevo quando se estabelece a importância dos intangíveis na economia empresarial, posicionando o investimento em activos intangíveis por oposição aos activos tangíveis. Estudos demonstram que os ativos intangíveis são fundamentais para o crescimento económico e empresarial (Haskel & Weslake, 2018; Stratone, 2023), especialmente dada a sua aceleração após a pandemia da COVID-19 (Hazan, 2021). No entanto, nem sempre foi assim, se revermos os estudos anteriores sobre intangíveis encontramos no início dos anos 90 a génese do conceito de CI.

Após a era pós-industrial dos anos 70, as empresas começaram a questionar-se sobre os activos intangíveis. Algumas décadas mais tarde, as economias globalizadas e em rede dos anos 90 demonstraram a importância do ativo incorpóreo de ter um fluxo interno e externo de informação, conhecimento acumulado e procedimentos próprios. Trata-se de activos intangíveis que não se reflectem nas demonstrações financeiras, mas que contribuem para a realização dos objectivos da empresa. Assim, podemos dizer que o CI surgiu como resultado da vontade de conhecer o produto resultante da subtração do valor real de uma empresa e do seu valor de mercado.

Edvinsson e Malone (1999), tentam explicá-la com a metáfora de que a QI seria as

raízes de uma árvore, algo que não se vê, mas que é necessário para o crescimento. Para esses autores, ela é composta pela infraestrutura, pelas relações com parceiros e clientes e pelas habilidades dos funcionários. Outros autores, como Johnson (1999), destacam neste grupo de intangíveis, a inteligência humana e a inovação como geradores de lucro. Uma revisão da literatura sobre QI leva-nos a extrair as teorias influentes como pilares do seu desenvolvimento:

1. *Visão baseada nos recursos (RBV)*. Barney (1991), postula que os recursos de uma empresa para serem competitivos devem ser valiosos, raros, inimitáveis e não substituíveis, popularizando no meio acadêmico e na prática, os chamados critérios RBV. Onde a estratégia empresarial se centra nas práticas e processos envolvidos na atividade diária desenvolvida na organização e nos seus resultados (Potter, 1996). Esta teoria vai começar a concetualizar não só os recursos tangíveis, mas também os recursos intangíveis como o conhecimento (Grant, 1996).

2. *Teorias da visão baseada no conhecimento (KBW)*. Na nova sociedade do conhecimento, este será o recurso por excelência. O seu principal exponencial é a espiral do conhecimento, amplamente popularizada pelos seus criadores, Nonaka e Takeuchi (1995). A sua visão da empresa é a de uma entidade ativa criadora e disseminadora de conhecimentos. Para o efeito, o conhecimento tácito, aquele que é inarticulado, intuitivo, surge do indivíduo com experiência "em" e "com" o trabalho que realiza "know how" (Nonaka & Takeuchi, 2021). É transmitido e, ao mesmo tempo, transformado na organização quando é aplicado (Grant, 1996) em conhecimento explícito. Pode ser codificado, escrito, objetivo e facilmente transferido (Nonaka & Konno, 1998), sendo o "saber sobre" criado a nível organizacional e individual. Esta teoria confere-lhe um dinamismo e uma projecção externa que faltavam à teoria anterior (Bontis, 2002).

3. *Teoria das capacidades dinâmicas*. Tal como referido pelos seus precursores (Teece et al., 1997), centra-se na capacidade combinatória das empresas para assegurar que os seus conhecimentos, competências e experiência permanecem incorporados nos seus produtos e processos e são difíceis de imitar. Embora mais moderna do que as anteriores, expandiu-se para os seguintes domínios: empreendedorismo (Alvarez & Barney, 2001); desempenho empresarial (Wang et al., 2011; Stratone, 2023); retorno do investimento (Chen et al., 2009; Tan et al., 2007); ambientes em rede (Zheng et al., 2011) e ambiente (Chen, 2008; Haarhaus & Liening, 2020).

Estas teorias resultam na definição de CI como o conjunto de recursos intangíveis e tangíveis e a capacidade das empresas para os gerir, tornando-as competitivas e sustentáveis.

2.1.1 Definição e dimensões do QI

A revisão da literatura não encontrou uma definição universalmente aceite de CI. Apesar disso, os autores concordam em mostrar como a sua identificação e utilização cria benefícios para a organização (Hazan et al., 2021; Sumedrea, 2013). Os contributos de alguns autores relevantes que investigaram o CI são apresentados de seguida (quadro 1).

Quadro 1

Principais contributos para as definições de CI.

Aportaciones a la definición del CI	Autor
Sistemas y procesos que la hacen competitiva.	Steward, 1997
Los activos que no están en los estados financieros pero deberían reflejarse.	Petty & Guthrie, 2000; Roos, 2001 Reed et al. 2006; HernandezBueno et al., 2008
Fuente de futuros beneficios.	Lev, 2001
Necesarios para la innovación.	López et al., 2004; Rideg et al., 2023
Impulsor de la innovación y factor clave en la economía.	OECD, 2006
Combinación de intangibles y tangibles alineados a la estrategia empresarial para generar beneficios.	Bueno et al., 2008
Conocimiento a disposición de la organización para decidir las estrategias.	Aramburu et al, 2015
Creación de valor	Cañibano et al., 2002 Demartinni & Trucco, 2016 Garanina et al., 2021
Motor del desarrollo económico y social	Merino et al., 2018 Suciu & Năsulea, 2018
Creación valor corporativo y generación ventajas sostenibles en economías emergentes	Xu & Wang, 2018
Recursos estratégicos.	García-Flores & Palma., 2020
Motor de la cuarta revolución industrial.	Li et al., 2020
La tecnología es impulsora de las relaciones sociales que posibilitan su difusión.	Briñez, 2021
Rápido crecimiento económico.	Hazan et al., 2021
Efectos en el valor del mercado	Dumay et al., 2016
Mejora el desempeño organizacional	Thum-Thysen et al., 2021 Fernández-Solís et al., 2025

Neste estudo, definimos o CI como valores intangíveis que, quando geridos em conjunto com valores tangíveis, contribuem para o crescimento empresarial, económico e social.

Tal como não existe consenso sobre a definição de QI, também não existe um modelo universalmente aceite para a sua medição. Ao longo do tempo, vários modelos tentaram classificar a medição dos intangíveis, evoluindo de modelos mais simples, como o Skandia (1997), para modelos mais complexos, como o modelo Intellectus atualizado (2011).

Entre os pioneiros na medição do QI, o Skandia Navigator de Edvisson e Malone (1997) agrupa os elementos que compõem o QI em duas dimensões para o seu estudo: o capital humano e o capital estrutural. Em contrapartida, na maioria dos autores que se dedicam ao estudo do CI, há consenso em agrupar os intangíveis que o compõem em três capitais: capital humano (CH), capital relacional (CR) e capital estrutural (CE) (Petty & Guthrie, 2000; Navarro & Medina, 2024). Para exemplificar, apresentamos as classificações em capitais com seus elementos no Quadro 2. A primeira coluna apresenta os indicadores de Johnson (1999) que contribuiu para a literatura com uma clara distinção entre indicadores financeiros e não financeiros em relação ao valor de mercado de uma empresa. A segunda coluna mostra a classificação feita por Cañibano et al. (2002) com base no projeto MERITUM¹ promovido pela OCDE e pela CE; foi representada porque a Instituição está enquadrada neste contexto.

Quadro 2
Exemplos de categorias de CI e classificações de indicadores.

Capitales	Elementos no financieros	Elementos CE y OCDE
Capital Humano (CH)	Habilidades; conocimientos; tareas y motivación	Capacidades, saberes, habilidades y experiencias
Capital Estructural (CE)	Procesos de negocio y renovación, flow de información, productos y servicios; formas de cooperación de procesos	Procedimientos, rutinas organizativas, cultura, sistemas, bases de datos, licencias, etcétera.
Capital Relacional (CR)	Relaciones con los socios, clientes, proveedores e inversores	Relaciones con clientes, proveedores, socios de I+D+i.

Para estes autores, o CI é a combinação dos elementos que compõem os capitais que as empresas possuem. No entanto, na revisão da literatura, encontrámos também autores como Delgado et al. (2008), que preferem estudá-lo dividindo-o em cinco dimensões: capital humano, capital tecnológico, capital organizacional, capital relacional e capital social. Seguindo esta última categorização do CI, poder-se-ia, portanto, considerar a conveniência de extrair o capital social do CI e de o alinhar com a economia social. A objeção que levantamos é que o capital social, quer como dimensão, quer como subdivisão do capital relacional, não cria, por si só, valor sem a interação dos outros dois capitais, como explicamos a seguir.

Para tal, neste ponto, definiremos de forma sintetizada as dimensões em que os elementos que compõem o QI são habitualmente categorizados pelos académicos para o seu estudo, e como estão relacionados:

- A dimensão capital humano (CH) compreende o conhecimento estabelecido nos funcionários de uma empresa; os indivíduos são capazes de gerá-lo (Delgado et al. 2008). Reside nas capacidades, competências, experiência (Bueno & Merino, 2007; Bellucci et al., 2021), valores e atitudes em relação à empresa e ao trabalho. Além disso, esse capital inclui o dos funcionários, pois eles são fontes

¹Measuring Intangible to Understand and Improve Innovation Management (MERITUM): projeto conjunto OCDE-CE para impulsionar a investigação na Europa (1998-2001).

ativas de conhecimento útil para a organização (Merino et al., 2018). A relação com os outros dois capitais manifesta-se tanto na inovação (Li et al., 2020), pois são os indivíduos de uma organização que solicitam novas formas de fazer as coisas (EC), como na capacidade de trabalhar com os outros e de negociar, o que requer motivação, lealdade e satisfação (EC, 2006) (CR).

- A dimensão capital estrutural (CE) é constituída, para a maioria dos autores (Chen et al., 2009; Delgado et al., 2008; Dumay et al., 2016; Merino et al., 2018, Oliveira et al., 2020), por ativos como: estrutura organizacional, rotinas, procedimentos, processos, bases de dados, manuais, patentes e softwares, que permanecem na empresa quando os indivíduos que nela trabalham terminam seu trabalho. Alguns destes activos são tangíveis, como as máquinas e a estrutura. No entanto, outros são intangíveis, como a propriedade intelectual, as marcas registadas, as patentes, a cultura organizacional (Chen et al., 2009) e a imagem (Merino et al., 2018; Jeffrey et al., 2019). A relação mais notável com os outros dois capitais baseia-se na estrutura da organização. Esta funciona como um andaime através do qual os processos e procedimentos são transferidos entre os capitais humano e tecnológico, criando relações entre as *partes interessadas*.²

- A dimensão do capital relacional (CR) abrange os ativos gerados pelo conjunto de relações entre funcionários, clientes, fornecedores, acionistas (Bellucci et al., 2021), alianças estratégicas que geram informações e conhecimentos relevantes para a empresa. A sinergia gerada com os outros capitais pode ser exemplificada pelas relações formais e informais entre os colaboradores da organização, pois são fundamentais na transmissão e geração de informação e conhecimento (CH). Com o EC, vemos isso através do fato de que esse conhecimento é disseminado de um indivíduo para outro e também é transformado ao permanecer nas organizações (De Castro & García, 2003), influenciando a economia e a sociedade (Garanina et al., 2021). A importância desse capital relacional é percebida na segmentação de clientes que as empresas costumam fazer; criando ou diminuindo acordos comerciais e estabelecendo ou fortalecendo alianças, já que nem todos têm as mesmas necessidades ou estas mudam ao longo do tempo.

Desta forma, é a interação dos capitais acima referidos que cria valor numa organização. Exemplificamos com a geração de conhecimento, pois este é reconhecido como fundamental para o desenvolvimento económico (OCDE, 2006). A informação e o conhecimento são disseminados através de estruturas humanas ou tecnológicas (Devenpor & Prusak, 2001; Wang, 2011) ou ambas (CH). Sabemos também que é acumulado nelas através de processos, operações, rotinas organizacionais, procedimentos, etc. (De Castro & García, 2003), estes são os andaimes para as actividades empresariais e sociais, alcançando valor organizacional (Demartinni & Trucco, 2016) (CE). Pois bem, em maior ou menor grau, é incentivado o desenvolvimento de uma rede, promovendo esquemas de participação, colaboração, desenvolvimento de iniciativas e plataformas sociais (CR). No entanto, essa rede, mesmo em seu estado ótimo, pode

² *Stakeholders*. Para o pioneiro Friedman, as *partes interessadas* são qualquer tipo de pessoa que influencia ou é influenciada por uma empresa. Os stakeholders da Guardia Civil incluem cidadãos, administrações públicas, guardas civis e outras organizações como ONG, segurança privada, universidades e forças policiais internacionais. Entre estes encontram-se também pessoas com interesses opostos que pertencem a: bandos criminosos, grupos terroristas, criminosos, etc.

dificultar o fluxo de conhecimento, devido aos elementos que a compõem, tais como: ter pessoal insuficiente ou ruim, má gestão, ou mesmo que os procedimentos ou políticas da estratégia da empresa interfiram negativamente nela (Merino et al., 2018).

Como conclusão teórica, não há dúvida de que a concentração no valor real de uma empresa e a sua determinação foram o *motor* do desenvolvimento do capital intelectual. O objetivo era explicar o resultado da diferença encontrada entre o valor de uma empresa nos seus livros financeiros e o seu valor de mercado. Este valor, explicado ao CI, deve-se à interação dos elementos que o formam, tais como: as competências, os conhecimentos e a experiência dos trabalhadores, juntamente com os projectos de I&D&I; as rotinas organizacionais; a interação das relações internas e externas (Briñez, 2021), tanto ao nível dos trabalhadores como dos fornecedores, acionistas, aliados e clientes (CE, 2006)³. Sem esquecer a gestão da sua transformação, aquisição e aplicação num ambiente em mudança (Nonaka & Takeuchi, 2021).

Estas características posicionam o CI como uma chave para o crescimento económico (Bellucci et al., 2021), social e sustentável (Secundo et al., 2020) adaptado a um mercado volátil, difuso, incerto, ambíguo, complexo (Nonaka & Takeuchi, 2021) e tecnologicamente disruptivo (Wang et al., 2021). Por este motivo, na secção seguinte iremos explicar empiricamente, através da instituição da Guarda Civil, como as empresas podem proporcionar benefícios económicos sociais através do CI.

2.2. A ECONOMIA SOCIAL E O CORPO INSTITUCIONAL DA GUARDA CIVIL

A economia social⁴ é definida como um conjunto de actividades empresariais e económicas realizadas por entidades para a realização do bem coletivo dos seus membros, o interesse económico geral e/ou social seguindo os princípios da economia social (MITES, 2025). Atualmente, o conceito está consolidado em Espanha e é difundido pelo Centro Internacional de Investigação e Informação sobre a Economia Pública, Social e Cooperativa. Se relacionarmos estes termos: público, social, cooperativo e economia pública, isso leva-nos a pensar numa organização que os alinhou na sua estratégia durante mais de 181 anos de existência: a Instituição da Guarda Civil, ao fazer convergir práticas económicas e sociais na prestação de bens e serviços. Apoiamo-nos no facto de encontrarmos na Instituição, princípios consagrados da economia social e colaborativa como os que a seguir se enumeram, de autores como Díaz-Foncea et al:

- Promover a solidariedade entre os trabalhadores, facilitando as estruturas e motivando-os para a solidariedade e a cooperação.
- Reconhecimento da solidariedade e do trabalho empenhado através do espírito de mérito.
- Promoção da igualdade em sentido lato e não apenas em função do género.
- Inclusão e coesão social.
- Ajudar e apoiar os grupos mais vulneráveis e as pessoas em risco de exclusão social.

³Documento RICARDIS da UE (2006). A Comissão Europeia baseia-se nesta interação com base no projeto MERITUM, 2002. É definida como a combinação de recursos e actividades de capital humano, capital estrutural e capital relacional de uma organização.

⁴ Está atualmente a ser promovido pelo Comité Económico e Social Europeu, centrando-se na interdependência entre a economia e a sociedade.

- Conciliação da vida profissional e familiar.
- Gerar sustentabilidade a nível interno e externo, com um claro respeito pelo ambiente e pela proteção da biodiversidade.

A vantagem competitiva desta Instituição é oferecer serviços de qualidade superior, de modo a ser uma referência no seu sector, perante os cidadãos, o Estado e a União Europeia. A sua missão, no seio das Forças e Corpos de Segurança do Estado, é "*proteger o livre exercício dos direitos e liberdades e garantir a segurança pública*" (Art. 104º, Constituição). Para tal, coloca as pessoas no centro da sua ação, garantindo a sua segurança e integridade, de forma próxima. As funções são apresentadas no quadro 3.

Quadro 3

Definição das competências funcionais da Guarda Civil

Nota: Os dados deste quadro baseiam-se na Lei Orgânica 8/1986, de 13 de março, e nos Relatórios de Sustentabilidade da Guardia Civil, 2023.

Para além das funções apresentadas no quadro anterior, através da partilha de competências com outras forças policiais regionais e nacionais, a Guardia Civil é responsável pela segurança dos cidadãos em 84,53% do território nacional e mar

Diferentes Cuerpos de Seguridad Artículo 11 (página 26)	Específicos de la Guardia Civil Artículo 12, B (página 27)
• Velar por el cumplimiento de las leyes y disposiciones generales. • Auxiliar y proteger a personas y bienes. • Vigilar y proteger edificios públicos. • Mantener el orden y velar seguridad ciudadana. • Prevenir la comisión de actos delictivos. • Investigar delitos, asegurar las pruebas e instrumentos poniéndolos a disposición del juez. • Prevención de la delincuencia. • Colaborar con Protección Civil, caso grave de riesgos o catástrofes.	• Control de armas y explosivos. • Resguardo Fiscal del Estado (costas, fronteras, puertos y aeropuertos) • Vigilancia del tráfico, tránsito y transporte en las vías públicas interurbanas (exceptuando el País Vasco y Cataluña). • Conservación de la naturaleza y medioambiente, recursos hidráulicos, riqueza forestal y de otra índole relacionada con la naturaleza. • Conducción interurbana de presos y detenidos. • Aquellas otras que les atribuye la legislación vigente.

territorial (CG, 2023). Por outro lado, enquanto força de segurança pública de natureza militar, pode realizar missões internacionais, integrando uma organização internacional como a EUROPOL, a ONU ou a NATO, bem como as Forças Armadas espanholas (CG, 2023).

Podemos dizer que, com mais de 80.000 efectivos, espalhados por todo o território nacional e internacional. Está diversificada em especialidades: Proteção da Natureza, Polícia Judiciária, Serviços de Informação e Serviço Marítimo, entre outras. Juntamente com o potencial humano destacado na segurança do cidadão, com mais de 2.000 unidades territoriais (GC, 2025).

2.2.1 Valor social criado pela instituição.

O valor social pode ser definido como o resultado positivo das acções desenvolvidas por uma entidade na sociedade (Retolaza & Alzola, 2021). Este valor intangível é contextualizado no compromisso da Guarda Civil em ir além do cumprimento da sua missão. Fazem-no como uma contribuição social, centrando-se tanto na melhoria da vida e no apoio aos cidadãos, como na consciência das preocupações ambientais, seguindo um dos princípios da economia social enunciados por Díaz e Lejarriaga (2019). Por exemplo, no que diz respeito a este último princípio, registou a sua pegada de carbono no Gabinete Espanhol de Alterações Climáticas (OECC), tornando-se uma das únicas forças policiais a fazê-lo a nível mundial. Destacamos também o prémio concedido pelas Nações Unidas em 2023, "Prémio de Proteção da Camada de Ozono para os Funcionários das Alfândegas e da Polícia".

Estes valores são potenciados pela Instituição através da transparência e reconhecimento das suas acções, apresentando um impacto integrador e colaborativo, onde as comunidades onde são desenvolvidos os seus projectos têm um papel na tomada de decisão, sobre o que consideram como valor. Portanto, a Instituição combina seus recursos, políticas e processos para alcançar melhorias na vida das pessoas e da sociedade em geral, que é o que se chama de valor social (Retolaza & Alzola, 2021).

Para desenvolver as suas capacidades, o seu modelo de negócio consiste em divulgar e aplicar uma cultura de segurança de qualidade, versátil, disponível e próxima do cidadão. Para tal, transmite o seu conhecimento e experiência a outras forças policiais nacionais e internacionais, aos cidadãos, ao governo e a outras partes interessadas, com profissionalismo e um carácter benevolente. Este último é reconhecido porque os guardas civis trabalham com o conhecimento e o empenho para fazer coisas extraordinárias, contribuindo para aquilo a que chamámos intangíveis.

Recorde-se que no primeiro Regulamento de Serviço de 1844, o artigo 32º já afirmava a sua natureza caritativa e protetora. Ao mesmo tempo, o artigo 6.º do Estatuto da Guardia Civil estabelecia que a Guardia Civil devia cuidar dos desprotegidos e ser um prognóstico feliz para os aflitos (CG, 2025). Alguns anos mais tarde, em 1929, a Instituição foi agraciada com a Grã-Cruz da Ordem Civil da Caridade, com um distintivo preto e branco, que implica risco pessoal, em reconhecimento dos serviços humanitários e heróicos prestados. Assim, podemos dizer que a solidariedade e a cooperação são valores que estão no ADN da Instituição desde a sua criação, tornando-se a marca da identidade do Instituto.

O espírito, ou carácter benevolente, ainda hoje está presente, expresso no seu Código de Conduta⁵. O artigo 21º estabelece a prestação de assistência aos cidadãos, quer o seu pessoal esteja ou não em serviço. Encontra-se também no ponto 7 do decálogo dos membros da Guardia Civil, que afirma que devem ajudar sempre os que mais precisam, concentrando-se nas pessoas em situações de vulnerabilidade e falta de proteção; está também expresso nos seus relatórios de responsabilidade social corporativa (MRSC) e na revista oficial da Guardia Civil.

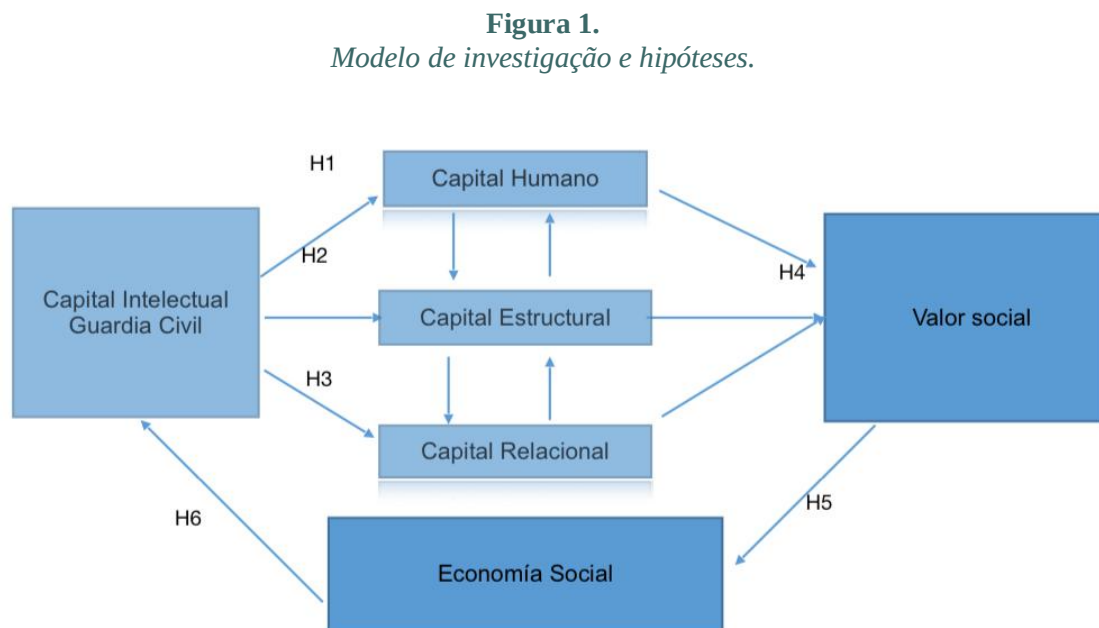
⁵ Decreto Real 176/2022, de 4 de março, que aprova o código de conduta da Guarda Civil.

Assim, este intangível é promovido pela Instituição, sendo considerado um ativo organizacional, promovendo-o através de serviços humanitários, do voluntariado, da luta pela biodiversidade e pelo ambiente. É produzido, quer a nível individual, quer noutras organizações, conforme consta no seu site #GComprometidos.

Face ao exposto, podemos afirmar que a missão da Guarda Civil não se baseia apenas na segurança pública, mas inclui também o bem-estar da sociedade, que é determinado através do dinamismo proporcionado pelas dimensões do CI que a constituem, gerando crescimento económico (Nonaka & Takeuchi, 2021). No entanto, este valor económico-social não é tido em consideração ou é desconhecido no meio académico, uma vez que, quando realizámos a nossa pesquisa, não encontramos nenhum estudo, investigação ou artigo sobre o tema. Por isso, na secção seguinte, vamos expor as nossas hipóteses sobre a contribuição do valor económico social da instituição no modelo de investigação.

3) METODOLOGIA

Com base no exposto, apresentamos o modelo de investigação (Figura 1) onde são definidas as hipóteses deste estudo:



H1. O Capital Humano está identificado na Instituição.

H2. O Capital Estrutural é identificado na Instituição.

H3. O Capital Relacional é identificado na Instituição.

H4. A inter-relação dos três capitais tem impacto na criação de valor social.

H5. O valor social gerado influencia a economia social.

H6. A economia social influencia o capital intelectual da Guardia Civil.

Para testar as nossas hipóteses, seguimos as indicações de Codina et al. (2020), realizando uma revisão da literatura utilizando bases de dados científicas como a SCOPUS, Web of Science e Google Scholar. Estes autores mostram na sua investigação que estas bases de dados, utilizadas pela comunidade científica internacional, cobrem amplamente todas as áreas do conhecimento. A pesquisa foi efectuada tanto nos campos: títulos dos artigos, no *resumo* ou através das palavras-chave indicadas neste artigo. No entanto, a pesquisa não obteve nenhum resultado, demonstrando a inexistência de artigos científicos sobre o nosso tema de investigação. Por esta razão, os nossos dados foram obtidos a partir da revisão documental e bibliográfica das bases de dados do Ministério da Administração Interna, bem como do Ministério da Defesa e da Instituição da Guarda Civil, onde a Instituição publica os seus relatórios financeiros e não financeiros. Por conseguinte, baseamo-nos em dados quantitativos e qualitativos de fontes primárias abertas.

A técnica escolhida foi a análise de conteúdo⁶, pois tem sido utilizada com frequência e sucesso na análise de relatórios de divulgação de CI (Magau 2021; Dumay et al., 2016). É também adequada para verificar hipóteses dedutivamente declaradas (Bini & Giunta, 2017). O corpus da análise de conteúdo, são os Relatórios de Responsabilidade Social da Guarda Civil (MRSCGC) e os Relatórios de Sustentabilidade (MS). A nossa decisão baseia-se no facto de os relatórios anuais serem ferramentas utilizadas pelas organizações para comunicar a todos os stakeholders o que consideram importante, divulgando-os nos mesmos (Petty & Guthrie, 2000; Bontis 2002; Guthrie & Abeysekera, 2006; Dumay et al., 2016). Em linha com a tendência atual de as empresas divulgarem as suas demonstrações financeiras e não financeiras às partes interessadas nestes relatórios anuais (Dumay et al., 2016).

Trata-se de um estudo longitudinal que abrange o período de 2014 a 2023, data dos últimos relatórios anuais de informação publicados. Para além de determinarmos a consistência dos dados, podemos obter a tendência institucional através da análise dos mesmos. Pretendemos responder se a contribuição da instituição para a economia social lhe é inerente, seguindo o nosso objetivo de estudo.

A unidade de análise na análise de conteúdo é aquela que indica a presença ou ausência dos elementos a serem investigados (Moreiro et al., 2006). Para obter esta unidade de análise, de entre os quadros conceptuais utilizados para definir, classificar e registar a informação divulgada no CI, alguns autores utilizam habitualmente o modelo de Sveiby (1997) modificado por Petty e Guthrie (2000). No entanto, nesta investigação, para obtermos a nossa unidade de análise, adaptámos os indicadores do modelo Intellectus⁷ (2011) à Instituição, devido à sua ampla repercussão nacional e internacional e por ser considerado um modelo integrativo de medição do QI (Merino et al., 2018). As considerações mais notáveis deste modelo são:

⁶ Para Allport (1965), é um método de estudo e análise das comunicações de forma sistemática, objetiva e quantitativa, com o objetivo de medir variáveis.

⁷ Documento Intellectus, nº5 (2003): Foi desenvolvido pelo Professor Bueno e pelo Centro de Investigação sobre a Sociedade do Conhecimento (CIC). Foi modificado em 2011, dando origem ao Modelo Intellectus: Medição e Gestão do Capital Intelectual, pelo IADE (Instituto de Administração de Empresas). Os indicadores adaptados são retirados do seu ponto 6. Tabela de indicadores (pp. 36-58).

- A criação de uma "árvore de relevância" que estabelece uma estrutura do CI, de forma a identificar as unidades de medida que o compõem, estabelecendo uma hierarquia de componentes, elementos, variáveis e indicadores. Nesta base, as categorias, os elementos, as suas definições e os indicadores foram adaptados para a identificação do CI na Instituição (Ver Anexo I: quadros 4-6).
- A elaboração de um Índice Sintético, baseado nos principais componentes para o quantificar. Estes são representados num "mapa de variáveis e principais indicadores" que será utilizado como medida quantitativa do conjunto de activos incorpóreos identificáveis. A seguir a este ponto, indicamos no Anexo II as fórmulas utilizadas para obter os índices.
- A elaboração do Relatório do CI (RCI), para a sua divulgação. Assim, seguindo a literatura, foi efectuada uma revisão dos documentos onde a Instituição divulga os seus relatórios financeiros e não financeiros.

Conseguimos limitar a subjetividade que poderia ocorrer na obtenção da unidade de amostragem ou unidade de análise, acrescentando transparência na categorização e utilizando regras de decisão consistentes ao longo do nosso estudo longitudinal. Em relação à fiabilidade, o instrumento de codificação foi manual, sem recurso a software, evitando os problemas apresentados por palavras com múltiplos significados que, embora possam ser reduzidos através do aumento das palavras-chave no contexto, não detectam o significado do CI específico da instituição, nem a interpretação que dele é feita (ver Anexo III: Fases da análise de conteúdo).

De seguida, para compreender o comportamento das nossas variáveis de estudo (dimensões do QI), categorizámo-las de acordo com a divisão tripartida do QI: capital humano, capital relacional e capital organizacional. Baseamo-nos nesta divisão tal como foi estabelecida pela Comissão Europeia (2006), com base no projeto MERITUM (Cañibano et al., 2002) citado na secção 2.2 (ver Anexo I: quadros 4-6).

Por fim, procedeu-se a uma análise estatística das medidas de distribuição de frequências, tendências e dispersão. O estudo estatístico tem como objetivo observar a importância dos elementos para a Instituição e a sua comparação e posição relativamente aos restantes elementos do CI, ao longo do período estudado. Para o efeito, foi utilizado o programa estatístico RStudio, versão 2024.12.0+467 para macOS 13+.

4. RESULTADOS E DISCUSSÃO

Os resultados da nossa investigação identificam a QI na instituição. Na análise da nossa investigação, adaptando o modelo Intellectus, as categorias, elementos e indicadores, a identificação dos seus elementos componentes deriva da construção das categorias, elementos e indicadores. O CI da Instituição pode ser classificado através do agrupamento dos seus elementos componentes em capital humano, capital estrutural e capital relacional (ver Anexo I). Estes resultados são semelhantes à maioria dos estudos académicos. Por conseguinte, aceitamos as três primeiras hipóteses desta investigação:

H1. O Capital Humano está identificado na Instituição.

H2. O Capital Estrutural é identificado na Instituição.

H3. O Capital Relacional é identificado na Instituição.

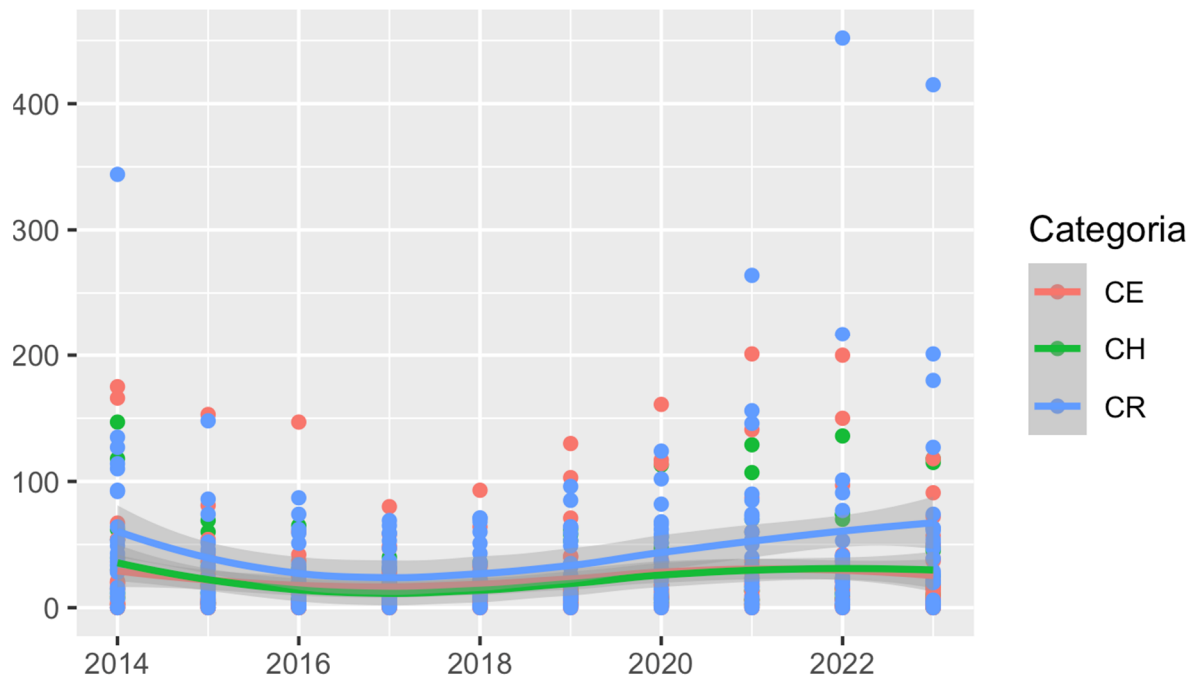
De seguida, procede-se à verificação das restantes hipóteses. No que se refere ao valor social, ao analisarmos a temática dos elementos que compõem os capitais do CI e os capitais da Instituição (Anexo I), verificamos que as definições dos elementos que compõem o capital humano, relacional e estrutural têm um impacto direto no valor social. Em outras palavras, os elementos do CI estão alinhados com a identificação do valor social na literatura, como mostra a tabela 7 abaixo.

Quadro 7
Relação entre o QI da instituição e o valor social.

Dimensión Capital Humano			
Elementos	Definiciones	Capital Humano	Valor social
IDENTIDAD MOTIVACIÓN CREATIVO EDUCACIÓN ESPECIALIDAD; UNIVERSITARIO FORMACIÓN EXPERIENCIA DESARROLLO APRENDIZAJE CIVIL CONCILIA LIDERAZGO	Valores, motivación a la excelencia en sus actuaciones, formación especializada y conocimientos. Adaptación y generación ideas novedosas aplicables en el desarrollo del trabajo.	Autores como Nonaka y Takeuchi (2021) puntualiza que las empresas que cuentan con empleados con muchas habilidades y experiencia son capaces de gestionar escenarios cambiantes. Capacidad sin actitud o aptitud generaría una desaceleración o destrucción del valor (Merino et al., 2018)	Valor aportado por las personas a las empresas (Carina et al., 2024). Las creencias personales sobre un propósito social (Díaz-Foncela et al., 2016).
Dimensión Capital Estructural			
Elementos	Definiciones	Capital Estructural	Valor social
CULTURA CLIMA IGUALDAD ESTRUCTURA DESARROLLO RUTINAS RELACIONINT CRIMINAL PROVEEDORES INVERSIONIDI PERSONALIDI INFRAESTRUCTURA EQUIPOPOLICIAL INNGEST COMUNICACIONGC MARCA LICENCIAS SECRETO PATENTES TECNOEXT TECNOEW TECLIC PLEXBIBILIDAD TALENTOS	Cultura institucional, idiosincrásica de la institución. Espíritu benemérito transferido generación a generación a través de acciones solidarias de cooperación, sacrificio y apoyo al necesitado. Seguridad y protección según la legislación vigente. La estructura de la Institución la hace distintiva, por su diversificación tanto geográfica como en especialidades para llegar a todos los ciudadanos. Andamiaje a través del cual el conocimiento, la experiencia y la información se transfiere diversificándose en especialidades aumentando así su valor empresarial. Sin olvidar las políticas e inversión en innovación y desarrollo.	Las empresas deben desarrollar su capital humano con los medios necesarios que apoye la visión sobre lo que las personas son capaces de hacer para generar cambio (Mohdzaini, 2021).	Recursos que los individuos pueden conseguir a través de la estructura de una organización (Sánchez et al., 2018). Sin estructuras sociales es difícil generar el capital social (Nonaka & Takeuchi, 2021).
Dimensión Capital Relacional			
Elementos	Definiciones	Capital Humano	Valor social
CIU LEALCIU QUEJAS PROTCIU ESTADO IADMINISTRACIÓN CAPITALEXTERIOR ALIANZAS ALIANZASESTABLES ALIANZASBENEFICIO CONCOMPETENCIA PRIVADA CERTICAL REDES ADMINISTRACIÓN MEDIOS DEFENSAMBIENTE VERDE MERCADO CODIGOCON ACSOCIAL BUENGOBIERNO	Genera valor a través de las relaciones y alianzas establecidas con todos sus grupos de interés. En el plano internacional, establece relación de cooperación y colaboración con otros países. Es reseñable el apoyo a los más vulnerable y desfavorecidos. La inclusión y la cohesión social. Impulsa proyectos de voluntariado dentro y fuera de la institución. Dedicada a la defensa del medioambiente interna y externamente y la biodiversidad. Cuenta para ello con una red de medios de comunicación internos y externos promoviendo la transparencia y el buen gobierno.	Las empresas generan valor a través de las relaciones creadas con sus grupos de interés (Maqbool,2020) y en la transmisión de ese conocimiento (Rideg et al. 2023; Nonaka & Takeuchi, 2021). Este conocimiento debe ser fluido (Merino et al., 2018).	A través de promover el empleo, la inclusión social, sostenibilidad, innovación y crecimiento económico se consigue impulsar la economía social (cepes, 2023). Las empresas logran sus objetivos sociales promoviendo la transparencia (Sumedrea, 2013). Los programas de inclusión económica tienen un fuerte impacto en las personas más pobres del mundo (Word Bank, 2024).

Uma vez quantificados os dados (Anexo II) para conhecer o comportamento dos elementos das nossas variáveis e saber se são constantes ao longo do período estudado, foi efectuada uma análise da distribuição de frequências e das medidas de tendência (Figura 2).

Figura 2
Distribuição de frequências e tendências dos elementos de CI (2014-2023)



A Figura 2 mostra como os elementos estão representados no período estudado, e sua distribuição em categorias. Nota-se que, enquanto a curva de dispersão do capital humano (CH) e do capital estrutural (CE) estão quase alinhadas ao longo dos 10 anos, indicando a constância entre as frequências dos elementos de ambos os capitais, a do capital relacional (CR) permanece acima delas. Além disso, as pontuações outlier dos elementos deste último capital são as mais afastadas em comparação com os outros dois capitais nos últimos anos, mostrando a relevância destes elementos.

De seguida, para determinar o agrupamento destes elementos, na figura 3, foram utilizadas medidas de tendência central e de posição. Foi elaborado um gráfico de caixa para visualizar tanto as medidas de posição central (média, mediana e moda) como as medidas de posição não central, os quartis, com base no conhecimento da dispersão dos dados da figura 2.

A Tabela 8 mostra a relevância dos elementos que obtiveram as pontuações mais altas: Parcerias estáveis, Parcerias benéficas, Proteção, Social, Verde, Defesa ambiental, no âmbito do CR. Os elementos: Penal, Comunicações, Igualdade, no âmbito do CE e os elementos: Formação, Desenvolvimento, Universidade e Criatividade, no âmbito do CH. Pontuações elevadas para os elementos: Protciu, juntamente com Asocial, durante 7 anos, Penal, durante 8 anos, e Comunicação, durante 10 anos.

Com estes dados (tabela 8) e as unidades amostrais (anexo I), podemos inferir que, para a instituição, as suas acções visam a segurança, a proteção dos cidadãos e o desenvolvimento de acções sociais através da força de parcerias e serviços conjuntos com outras identidades. Na mesma linha, as suas acções visam a proteção do ambiente e da biodiversidade. Para ela, o "valor" não é apenas considerado em termos financeiros, mas, na linha de Nonaka e Takeuchi (2021), o "social e o ambiental" são também activos valiosos, e ela é constante nisso. Para o efeito, o seu capital humano é igualitário e diversificado, qualificado e desenvolvido, adaptando-se e criando novas ideias no desempenho do serviço através da transferência do seu conhecimento.

Esses resultados mostram que a definição de valor social segue a definição de valor social como um resultado gerado a partir da combinação de recursos, processos e políticas que melhoram a vida das pessoas e da sociedade como um todo (Sánchez et al., 2018). Portanto, vemos que a hipótese 4 é corroborada:

H4: A interação destes capitais gera valor social.

Seguindo a nossa linha de investigação, vamos agora averiguar de que forma este valor social tem impacto na economia social, para além da sua missão principal, descrita na secção 2: Proteção e Ação Social ao cidadão (quadro 9), seguindo os princípios da economia social e a definição de valor social.

Quadro 9

Indicadores dos elementos: proteção e ação social para os cidadãos.

Os dados acima apresentados (quadro 9) são interessantes, pois indicam que, nos últimos nove anos, foram realizados 1 883 862 serviços humanitários; 14 689 acções em

	2022	2021	2020	2019	2018	2017	2016	2015	2014
Acciones beneficio comunidad (más allá misiones encomendadas).	1.012	960	1.151	2.659	2.647	2.986	1.956	1.318	1.620
Acciones solidarias (voluntariado nivel individual hay constancia).	1.026	267	347	121	114	140	215	180	62
Actividades de acercamiento a la sociedad	247	499	503	482	340	316	105	904	142
Charlas en centros escolares	34.459	21.328	16.078	34.848	12.970	12.412	16.245	12.814	11.782
Acciones seguridad mayores	3.607	2.740	3.275	3.732	3.816	3.769	9.712	10.364	11.605
Colaboraciones convenios.	261	149	106	114	92	86	96	115	95
Servicios humanitarios	242.575	218.303	215.697	194.923	193.593	193.135	458.360	167.266	SD

benefício da comunidade e 2 410 acções de voluntariado. Para além de outras actividades de solidariedade e proteção de idosos e menores. Demonstrando que as pessoas são mais importantes do que o capital na economia social (Pedreño, 2024).

Estes dados mostram que os serviços humanitários e as acções em prol da sociedade são uma mais-valia. Além disso, o seu valor económico é inestimável. Para visualizar o valor económico destas acções, resumimo-lo tomando como exemplo a Asociación Guardias Civiles Solidarios⁸ (ASGS). O quadro 10 apresenta o valor económico das suas acções nos últimos 5 anos, dados obtidos a partir dos relatórios anuais da ASGC.

Quadro 10
Avaliação económica das acções "Guardas Civis Solidários"

Com os dados apresentados em ambas as tabelas (8 e 9) entramos na disciplina da

	Actuaciones	Niños	Adultos	Alimentos (kg.)	Valor económico €
Memorias 2024	60	2.977	2.987	22.540	60.257
Memorias 2023	44	4.771	9.109	44.980	45.396
Memorias 2022	65	1.832	63.396	362.040	367.356, 21
Memorias 2021	54	2.419	5.346	13.210	52.000
Memorias 2020	138	2.017	13.251	8.262	38.482

economia social que permeia a economia tradicional, o valor do social (Diaz-Foncea et al., 2016) e a instituição da Guardia Civil que a sustenta, através do seu capital intelectual. Assim, demonstra-se que o valor dos serviços prestados tem um impacto positivo na economia social, ao prosseguir o interesse económico e/ou social geral. Portanto, a hipótese 5 da nossa pesquisa é confirmada:

H5: O valor económico social da instituição influencia a economia social.

Por fim, analisámos se a economia social retorna à Instituição, completando assim o objetivo da nossa investigação. Para o efeito, analisámos a confiança concedida à Instituição por cidadãos, instituições e entidades diversas, realizada pelo Centro de Investigação Sociológica (CIS) durante o período estudado. Os resultados são apresentados no quadro 11.

⁸Em 2014, foi fundada a Asociación Guardias Civiles Solidarios (ASGC) com o objetivo de canalizar as numerosas acções individuais do pessoal voluntário.

Quadro 11
Valorização da instituição pela sociedade espanhola

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Posición entre instituciones más valoradas	SD	FFCCSE	FFCCSE	FFCCSE	1ª	1ª	1ª	1ª	1ª	1ª

Como podemos ver, uma valorização positiva é transmitida à instituição através da lealdade e confiança que a sociedade deposita nela. Ser reconhecida como uma instituição com valor social aumenta significativamente a sua reputação (Jeffrey et al., 2019; Maqbool et al., 2018). No seio da instituição, o compromisso adquirido pelos guardas civis com a sociedade favorece a autoestima e a motivação pela luta em prol dos direitos humanos e dos mais desfavorecidos (MS, 2023). Estas ações, programas ou projetos de voluntariado estão alinhados com os objetivos da instituição, como proteger e ajudar os cidadãos, fortalecendo-a.

Além disso, a sua estrutura e diversificação consolidada não só serve para alianças que geram redes sociais já estabelecidas, mas também facilita as ligações entre comunidades e indivíduos que estão distantes uns dos outros (Álvarez & Berni, 2001). Sem esquecer que a coesão e a confiança nelas geradas facilitam a disseminação interna e externa do conhecimento, que é um intangível valorizado na economia (Nonaka & Takeuchi, 2021), tornando-a mais competitiva.

De acordo com o que precede, a nossa última hipótese (H6) é verificada, concluindo assim o nosso objetivo de investigação.

H6: A economia social regressa à instituição.

5. CONCLUSÕES

Uma característica marcante do nosso tempo é a forma como as empresas gerem o capital social. A Instituição responde à questão colocada pela nova perspetiva económica onde as organizações reflectem sobre a sua contribuição de valor para a sociedade (Retolaza & Alzola, 2021). Ao analisarmos esta questão através do CI da Instituição Guarda Civil, que pertence ao sector público e é eminentemente social, defendemos que, tal como o capital não cria valor por si só, também os investimentos nele realizados não o fazem por si só. Serão as capacidades geradas pelas empresas na gestão destes intangíveis que permitirão o crescimento económico (Hazan et al., 2021), através dos serviços.

A Instituição, no exercício da sua atividade de segurança e proteção dos cidadãos, vai mais longe, criando melhorias na vida dos indivíduos e/ou da sociedade em geral. De acordo com os dados, isso deve-se ao conhecimento, às relações, à cultura organizacional, à experiência e à participação ativa das pessoas que compõem a instituição. Deduzimos, através dos resultados obtidos na investigação realizada, que cumpre um dos objectivos definidos no relatório da Parceria para a Inclusão Económica do Banco Mundial (2024), ao ser capaz de avaliar os seus programas sociais com base em evidências-chave.

As suas acções apresentam um modelo inclusivo, atingindo diretamente os mais necessitados, gerando coesão social através da estrutura institucional e da sua

diversificação. Tem uma estrutura sólida que é necessária para a colaboração com outras organizações não governamentais, comunitárias e do sector privado (García-Flores & Palma, 2019), reduzindo assim as limitações de capacidade.

O carácter meritório da instituição, impulsionado pelo seu pessoal, é um valor social, que é definido neste trabalho ao mostrar o impacto positivo das suas acções na sociedade. Ao mostrá-la como um ator ativo, abrimos uma brecha no estereótipo da segurança, indo mais longe com as suas acções sociais, a proteção do ambiente e a biodiversidade. Neste caso, apresentámos um modelo inclusivo que acredita que a solidariedade e a cooperação são necessárias, elimina barreiras sociais e transforma ambientes difíceis. Estes activos são valiosos para a Instituição, seguindo os critérios VRIN de Barney (1991), uma vez que são difíceis de imitar, comprar ou substituir, proporcionando uma vantagem competitiva.

Consideramos que os dados e os instrumentos de medição adequados são essenciais para a implementação de políticas corretas em qualquer tipo de capital. Isto permite obter informações e mostrar a todas as partes interessadas o investimento efectuado e os resultados obtidos (García-Porras, 2025), sob o prisma da transparência. Nesta investigação, foram recolhidos e analisados dados quantitativos e qualitativos, continuando linhas abertas de investigação baseadas em evidências sobre os diferentes ecossistemas que acolhem a economia social, cumprindo um dos objectivos da estratégia industrial definida pela UE (Carini et al., 2024).

Concluimos com os contributos e limitações encontrados neste estudo. Os resultados mostram, por um lado, que as instituições pertencentes ao sector público podem envolver-se com as organizações não-governamentais e privadas como um agente de mudança necessário, promovendo a economia social. Por outro lado, contribuimos para a aplicação do estudo da gestão do CI numa instituição pertencente ao sector público, uma vez que o estudo do CI está mais centrado no sector privado. Acreditamos que é inovador investigar o valor social numa instituição que é frequentemente estudada numa perspectiva legal ou operacional.

No que respeita às limitações encontradas, importa referir que o facto de os dados se basearem em documentos institucionais pode gerar um enviesamento de fonte única. Do mesmo modo, os índices dos elementos obtidos a partir do CI não foram ponderados, o que minimiza a importância relativa que podem ter para o grupo específico de peritos em economia social. Seria necessária mais investigação neste domínio para melhorar a nossa compreensão desta questão. Por conseguinte, uma futura linha de investigação poderia reforçar este estudo, recorrendo a opiniões de peritos e outras percepções externas e considerando a utilização de índices ponderados.

REFERÊNCIAS BIBLIOGRÁFICAS

- Alvarez, S. A., & Barney, J. B. (2001). How entrepreneurial firms can benefit from alliances with large partners. *Academy Of Management Perspectives*, 15(1), 139-148. <https://doi.org/10.5465/ame.2001.4251563>
- Aramburu, N., Sáenz, J. e Rivera, O. (2005). Gestão do Conhecimento: Aspectos metodológicos e empíricos. Documento de trabalho. San Sebastián, Universidade de Deusto EAST.
- Arteaga A. L., Ojeda, J. F., e Alvarez D. G. (2020). Trajetória e estratégias de empreendedorismo em mulheres. *aDRResearch ESIC International Journal Of Communication Research*, 22(22), 176-195. <https://doi.org/10.7263/adresic-022-10>
- Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99-120. <https://doi.org/10.1177/014920639101700108>
- Bellucci, M., Marzi, G., Orlando, B., & Ciampi, F. (2021). Uma revisão de temas emergentes e tendências futuras. *Journal of intellectual capital*, 22(4), 744-767. <https://doi.org/10.1108/JIC-10-2019-0239>
- Bini, L., Bellucci, M., & Giunta, F. (2017). Integrando a sustentabilidade na divulgação do modelo de negócios: Evidências da indústria de mineração do Reino Unido. *Journal of Cleaner Production*, 171, 1161-1170. <https://doi.org/10.1016/j.jclepro.2017.09.282>
- Briñez M. E. (2021). Tecnologia da informação: uma ferramenta de capacitação para a gestão do capital intelectual? *Revista de Ciencias Sociales* 27(1), 180-192. <https://dialnet.unirioja.es/servlet/articulo?codigo=7817690>
- Bontis, N. (2002). Intellectual capital disclosure in Canadian corporations (Divulgação do capital intelectual nas empresas canadianas). *Journal of Human Resource Costing and Accounting*, 7(1-2), 9-20.
- Bueno E. J. e Merino C. (2007). O capital intelectual e a criação de empresas na sociedade. *Encuentros multidisciplinares*, (9)26, 37-46. <https://dialnet.unirioja.es/servlet/articulo?codigo=2324790>
- Bueno, E. J., Salmador, M. P. e Merino, C. (2008). Gênese, conceito e desenvolvimento do capital intelectual na economia do conhecimento: Uma reflexão sobre o Modelo Intellectus e suas aplicações. *Estudos em Economia Aplicada*, 26(2), 43-63. <https://www.redalyc.org/pdf/301/30113187003.pdf>
- Burt, R. S. (2004). Brokerage and Closure: An Introduction to Social Capital. http://ronaldburt.com/research/files/B&C_Introduction.pdf

Cañibano L., Sánchez, P., García-Ayuso, M., e Chaminade, C. (2002). Projeto MERITUM. Diretrizes para a gestão e divulgação de informação sobre intangíveis (Intellectual Capital Report). Fundação Vodafone.

<https://dialnet.unirioja.es/servlet/libro?codigo=448252>

Carini, Ch., Galera, G., Tallarini, G., Chaves, A., Sak, B. & Schoenmaeckers, J., (2024). *Avaliação comparativa do desempenho socioeconómico da economia social da UE*. Comissão Europeia.

https://eisma.europa.eu/news/study-benchmarking-socio-economic-performance-eu-social-economy-now-published-2024-09-19_en

Comissão Europeia (CE, 2006). Reporting intellectual capital to augment research, development *and innovation in SMEs: report to the Commission of the High Level Expert Group on RICARDIS* (Comissão Europeia. Direção-Geral da Investigação ed.). Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias.

<https://op.europa.eu/es/publication-detail/-/publication/60cbf27c-5552-429f-a077-44135a97cc27/language-en>

Chen, Y. S. (2008). O efeito positivo do capital intelectual verde nas vantagens competitivas das empresas. *Journal of Business Ethics*, (77)3, 271-286. <https://doi.org/10.1007/s10551-006-9349-1>

Chen, H., Shih A. & S. Y. Yang, (2009). O papel do capital intelectual na transferência de conhecimentos. *IEEE Transactions on Engineering Management*, (56)3, 402-411.

<https://ieeexplore.ieee.org/abstract/document/5072284>

Codina, L., Morales-Vargas, A., Rodríguez-Martínez, R. e Pérez-Montoro, M. (2020). Uso de Scopus e Web of Science para pesquisa e avaliação em comunicação social. Análise comparativa e caracterização. *Index.Comunicación/Index Comunicación*, 10(3), 235-261. <https://doi.org/10.33732/ixc/10/03usodes>.

Davenport, T. e Prusak, L. (2001). O conhecimento em ação. Buenos Aires: Prentice Hall. Argentina.

De Castro, G. e García-Muiña, F. E (2003). Hacia una visión integradora del capital intelectual de las organizaciones. Conceito e componentes. *Boletim Económico ICE, Informação Comercial Espanhola*, 2756, 7-16. <https://dialnet.unirioja.es/servlet/articulo?codigo=303756>

Delgado, M., Navas, J.E., Martín. G. & López, P. (2008). A inovação tecnológica a partir do quadro do capital intelectual. Cuaderno de Trabajo 04/2008. Universidade Complutense de Madrid.

- Demartini, C., & Trucco, S. (2016). Does Intellectual Capital Disclosure Matter for Audit Risk? Evidence from the UK and Italy. *Sustainability*, 8(9), 867. <https://doi.org/10.3390/su8090867>
- Díaz B. F. e Lejarriaga G. (2019). Apresentação da monografia: Empreendedorismo social e empregabilidade. *REVESCO. Revista de Estudios Cooperativos*, 129, 9-15. <https://doi.org/10.5209/REVE.62962>
- Díaz-Foncela M., Marcuello S. e Monreal G. (2016). Economía social e economía colaborativa: Ajuste e potencialidades. *Economía Industrial*, 402, 27-35 <https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/402/D%C3%80DAZ%20FONCELA,%20MARCUELLO%20Y%20MONREAL.pdf>
- Dumay, J., Bernardi, C., Guthrie, J., & Demartini, P. (2016). Relato integrado: Uma revisão estruturada da literatura. *Accounting Forum*, 40(3), 166-185. <https://doi.org/10.1016/j.accfor.2016.06.001>
- Edvinsson, L. e Malone, M.S. (1999). *Capital intelectual*. Barcelona: Gestión, 2000.
- Fernández, D. J. Guevara, G. D., Dávila T. L. e Cruz, J. J. (2022). Capital intelectual como fator de desempenho organizacional em Micro e Pequenas Empresas. *Journal of Research in Communication and Development*, 13(1), 63-73. <https://doi.org/10.33595/2226-1478.13.1.595>
- Fernández-Solís, C., González-Ramírez, M. R., e Gascó-Gascó, J. (2025). A intenção de adoção da analítica de recursos humanos e o seu impacto no desempenho organizacional: uma abordagem teórica. *INNOVA Research Journal*, 10(1), 93-111. <https://doi.org/10.33890/innova.v10.n1.2025.2706>
- Garanina T., Hussinki H., & Dumay J. (2021). Contabilização de intangíveis e capital intelectual: uma revisão da literatura de 2000 a 2020, *Contabilidade e Finanças*, no prelo. <https://doi.org/10.1111/acfi.12751>
- García-Flores, V. e Palma Martos, L. P. (2019). Inovação social: factores-chave para o seu desenvolvimento nos territórios. *CIRIEC-Spain Revista de Economía Pública Social y Cooperativa*, 97, 245-278. <https://doi.org/10.7203/ciriec-e.97.14148>
- García-Flores, V. e Palma Martos, L. P. (2020). Entidades do terceiro sector e inovação social. Elementos caracterizadores e factores de sucesso. *Revista REVESCO de Estudios Cooperativos*, 136, e71861. <https://doi.org/10.5209/reve.71861>
- García-Porras, B. (2025). Apresentação do relatório estatístico CIRIEC, Euricse e Spatial Foresight. Benchmarking the socio-economic performance of the EU Social Economy. <https://ciriec.es/noticias/el-nuevo-informe-de-euricse-ciriec-internacional-y-spatial-foresight-impulsado-por-la-comision-europea-cifra-en-115-millones-las-personas-empleadas-en-la-economia-social-en-la-ue/>

- Grant, R. M. (1996). Toward a Knowledge-Based Theory of the Firm (Para uma teoria da empresa baseada no conhecimento). *Strategic Management Journal*, 17, 109-122. <https://doi.org/10.1002/smj.4250171110>
- Guthrie, J. & Abeysekera, I. (2006). Content analysis of social, environmental reporting: What is new?, *Journal of Human Resource Costing & Accounting*, 10(2), 114-126. <https://doi.org/10.1108/14013380610703120>
- Hazan, E., Smit, S., Woetzel J., Cvetanovski, B., Krishnan, M., Gregg, B., Perrey J. & Hjartar, K. (2021). Tornar tangível o intangível. The future of grow and productivity? Mckinsey Global Institute. <https://doaj.org/article/faecfbdaace64e669c135ccadc104776>
- Haarhaus, T. & Lienen, A. (2020). Construindo capacidades dinâmicas para lidar com a incerteza ambiental: O papel da previsão estratégica. *Technological Forecasting and Social Change*, 155. <https://doi.org/10.1016/j.techfore.2020.120033>
- Jeffrey, S., Rosenberg, S. & McCabe, B. (2019). Comportamentos de responsabilidade social corporativa e reputação corporativa. *Social Responsibility Journal*, 15(3), 395-408. <https://doi.org/10.1108/SRJ-10.11-2017-0255>
- Johnson, W.H.A. (1999). An integrative taxonomy of intellectual capital: Measuring the stock and flow of intellectual capital components in the firm. *International Journal of Technology Management*, 18(5-8), 562-575.
- Lev, B. (2001). *Intangibles: Management, Measurement, and Reporting*. Washington DC: Brookings Institution Press. <http://www.jstor.org/stable/10.7864/j.ctvcj2rf2>
- Li, X., Nosheen, S., Haq, N. U., & Gao, X. (2020). Criação de valor durante a quarta revolução industrial: Uso do capital intelectual pelas empresas mais inovadoras do mundo. *Technological Forecasting And Social Change*, 163, 120479. <https://doi.org/10.1016/j.techfore.2020.120479>
- López P., Martín de Castro, G., e Navas, J.E. (2004). Uma abordagem das relações entre os elementos do capital intelectual nas organizações. *Boletim Económico do ICE* (2817). <https://www.revistasice.com/index.php/BICE/article/view/3626/3626>
- Maqbool, S., Rasool, H., & Ahmad, S. (2018). Responsabilidade social corporativa e desempenho financeiro: uma análise empírica de bancos indianos. *Future Business Journal*, 4(1), 2314-7210. <https://doi.org/10.2139/j.fbj.2017.12.002>
- Magau, M. D., Roodt, G., & van Zyl, G. (2021). Uma escala de medição para avaliar a divulgação do capital intelectual. *Journal of HumanResource Management*, 19, 1-14. <https://doi.org/10.4102/sajhrm.v19i0.1645>
- Merino C., Alonso, M., González, N., & Plaz, R. (2018). Gestão do conhecimento em organizações do sector nuclear. Universidade Nacional de Educação a Distância (UNED).

- Ministério do Interior (GC, 2023). Relatório de Sustentabilidade da Guardia Civil 2023. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/memoria-RSC-Sostenibilidad-de-la-Guardia-Civil/Memoria-sostenibilidad-GC_126230302_pdfWEB.pdf
- Ministério do Trabalho e da Economia Social (MITES). Relatório de evolução e tendências no domínio da economia social (2023). Confederação Empresarial da Economia Social Espanhola (CEPES). https://www.fundae.es/docs/default-source/publicaciones-y-evaluaciones/publicaciones-econom%C3%ADa-social/1-1-evoluci%C3%B3n-y-tendencias-de-la-ec-social_2023.pdf
- Mohdzaini, H. (2021). A tecnologia e o futuro do trabalho: como a inteligência artificial (IA), os robôs e a automação estão a moldar o mundo do trabalho, as considerações éticas e o papel dos profissionais. CIPD. <https://www.cipd.org/uk/knowledge/factsheets/emerging-future-work-factsheet/>
- Moreiro J. A., Morato J., Sánchez S. y Rodríguez B. A., (2006). Categorização de conceitos em análise de conteúdo: a sua sinalização desde a Retórica clássica até aos Topic Maps. *Investigación Bibliotecológica: Archivonomía, bibliotecología e información*, 20(40). <https://doi.org/10.22201/iibi.0187358xp.2006.40.4097>
- Navarro González A. e Medina Jiménez, A., (2024). Relación del Capital intelectual con el capital humano, estructural y relacional. *Transcender Contabilidad y Gestión*, 9(26), 100-127. <https://doi.org/10.36791/tcg.v9i26.260>
- Nonaka, I. & Takeuchi, H. (1995). *The knowledge creating company*. Nova Iorque: Oxford University Press.
- Nonaka, I. & Konno, N. (1998). The Concept of Ba: Building a Foundation for Knowledge Creation. *California Management Review*, 40, 40-54. <https://doi.org/10.2307/41165942>
- Nonaka, I., & Takeuchi, H. (2021). Humanizando a estratégia. *Long Range Planning*, 54(4), 102070. <https://doi.org/10.1016/j.lrp.2021.102070>
- Oliveira, M., Curado, C., Balle, A. R., & Kianto, A. (2020). Partilha de conhecimento, capital intelectual e resultados organizacionais em PMEs: estão relacionados? *Journal of Intellectual Capital*, 21(6), pp. 893-911. <https://doi.org/10.1108/JIC-04-2019-0077>
- Organização para a Cooperação e Desenvolvimento Económico (2006). Criar valor a partir dos activos intelectuais. Reunião do Conselho da OCDE a nível ministerial.
- Pedreño, J., (2024). A economia social e os objectivos da UE 2024-2029. Europa Economia Social. <https://www.socialeconomy.eu.org/2024/10/22/great-sucess-of-the-event-the-social-economy-and-the-eu-2024-2029-objectives/>
- Petty, R., & Guthrie, J. (2000). Intellectual capital literature review. *Journal Of Intellectual Capital*, 1(2), 155-176. <https://doi.org/10.1108/14691930010348731>

- Porter, M. (1996). O que é estratégia? *Harvard Business Review* 74(6), 61-78. https://iqfystage.blob.core.windows.net/files/CUE8taE5QUKZf8ujfYIS_Readin+1.4.pdf
- Retolaza, J. e Alzola, M. (2021). Aplicação do valor social nas organizações. *Boletim de Estudos Económicos*, 76(232), 19-22. <https://doi.org/10.18543/bee.2383>
- Rideg, András, Szerb, László, & Róza Varga, Anna (2023). O papel do capital intelectual na inovação: Evidências das PME húngaras. *Tec Empresarial*, 17(2), 1-19. https://www.researchgate.net/publication/370608181_The_role_of_intellectual_capital_on_innovation_Evidence_from_Hungarian_SMEs
- Roos, J. (2001). *Capital intelectual: o valor intangível da empresa*. Barcelona: Paidós.
- Sánchez-Espada J., Martín S., Bel P. e Lejarriaga G. (2018). Educação e formação em empreendedorismo social: características e criação de valor social sustentável em projectos de empreendedorismo social. *REVESCO. Revista de Estudos Cooperativos*, 129, 16-38. <http://dx.doi.org/10.5209/REVE.62492>
- Secundo, G., Ndou, V., Del Vecchio, P., & De Pascale, G. (2020). Desenvolvimento sustentável, capital intelectual e políticas tecnológicas: Uma revisão estruturada da literatura e uma agenda de pesquisa futura. *Technological Forecasting And Social* <https://doi.org/10.1016/j.techfore.2020.119917>
- Stratone, M. (2023). Uma Análise Bibliométrica do Papel do Capital Intelectual na Agilidade e Desempenho Organizacional. *Proceedings Of The International Conference On Business Excellence*, 17(1), 1275-1285. <https://doi.org/10.2478/picbe-2023-011>
- Steward, T. (1997). *A nova riqueza das organizações: o capital intelectual* Buenos Aires: Ediciones Granica S.A.
- Suciu, M., & Năşulea, D. (2018). Capital Intelectual e Economia Criativa como Fatores Chave para a Competitividade Rumo a um Desenvolvimento Inteligente e Sustentável: Desafios e Oportunidades para as Comunidades Culturais e Criativas. In: *Intellectual Capital Management as a Driver of Sustainability*. https://doi.org/10.1007/978-3-319-79051-0_5
- Sumedrea, S. (2013). Capital intelectual e desempenho da empresa: uma relação dinâmica em tempo de crise. *Procedia Economics And Finance*, 6, 137-144. <https://www.sciencedirect.com/science/article/pii/S2212567113001251?via%3Dihub>
- Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533.
- Thum-Thysen, A., Voigt, P., & Weiss, C. (2021). Reflections on Complementarities in Capital Formation & Production: Tangible & Intangible Assets across Europe [Reflexões sobre as complementaridades na formação e produção de capital: activos corpóreos e incorpóreos na Europa]. Comissão Europeia/Economia

Europeia[em linha]https://economy-finance.ec.europa.eu/document/download/3ddd17a1-0d58-4614-a363-90a9e6a12e9c_en?filename=dp152_en.pdf

Wang, C.N., Chang, Y.L., Huang, Q.H. & Wang, C.H. (2011). Avaliação da gestão do capital intelectual na indústria farmacêutica de Taiwan: utilização de GRA e MPI. *Jornal Africano de Gestão Empresarial* 5(7), 2950-2958.

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=78a492920f297eb118e7972ef4ad52ce99ec2355>

Grupo do Banco Mundial (2024). Relatório Anual 2024. <https://openknowledge.worldbank.org/bitstreams/91a20260-c3c4-4ed7-a488-d7dd8d419c8a/download>

Xu, J., & Wang, B. (2018). Capital intelectual, desempenho financeiro e crescimento sustentável das empresas: evidências da indústria de manufatura coreana. *Sustainability*, 10(12), 4651. <https://doi.org/10.3390/su10124651>.

Zheng S., Zhang W., Wu X. & Du J. Know ledge-based Dynamic capabilities and innovation in networked environments. *Journal of Knowledge Management* 15(6), 1035-1051.

Anexo I

Quadros 4-6: Unidades de amostragem e definição das dimensões de QI na instituição

ELEMENTOS DIMENSIÓN CAPITAL HUMANO		
Códigos	Unidad Muestral	Definición
CHIDENTIDAD	Pertenencia y compromiso.	Identificación de las personas como guardias civiles dentro de la Institución.
CHMOTIVACION	Automotivación	Los impulsos conscientes que hacen a los guardias civiles conseguir desempeñar el servicio con excelencia.
CHSATISFACCION	Satisfacción	Forma de participar en el desempeño de su trabajo y comportamientos de los guardias civiles en la Institución. Evaluación desempeño.
CHCREATIVO	Creatividad. Cultura innovadora	Creación de ideas nuevas y aplicables al desempeño del servicio. La forma de impulsar los pensamientos nuevos, ideas y actitudes por la Institución para generar nuevas formas de actuación o una mejora de las existentes.
CHEDUCACION	Educación reglada.	Conocimientos explícitos que posee en general los guardias civiles.
CHESPECIALIDAD	Formación especializada.	Conocimientos específicos de una especialidad concreta o trabajo técnico en la Institución
CHUNIVERSITARIO	Inversión en formación Universitaria.	Centro Universitario Guardia Civil (CUGC).
CHFORMACION	Formación interna.	Conocimientos adquiridos mediante programas, jornadas, talleres, y todos los cursos de formación que comprenden la capacitación y promoción interna en las Academias y en el Centro Universitario de la GC.
CHEXPERIENCIA	Experiencia.	Conocimientos adquiridos mediante el desempeño realizado en la Institución.
CHDESARROLLO	Desarrollo personal.	Conocimientos adquiridos informalmente en la Institución. Personas que promocionan. Promoción interna.
CHAPRENDIZAJE	Aprendizaje	Adquisición de nuevos conocimientos. Jornadas PATIO Y SIO.
CHCIVIL	Colaboración, personal civil.	Capacidad de trabajar con otras personas: compañeros, personal administraciones públicas. Personal civil funcionariado.
CHCONCILIA	Conciliación vida familiar profesional	Favorecer el equilibrio entre la vida familiar y la laboral a los guardias civiles. Compatibilizar la vida profesional y familiar.
CHLIDERAZGO	Liderazgo.	Guiar y mover a los compañeros hacia el desempeño de un servicio con excelencia y otras personas relacionadas con el servicio.

ELEMENTOS DIMENSIÓN CAPITAL ESTRUCTURAL

Códigos	Unidad Muestral	Definición
CECULTURA	Homogeneidad cultural.	Aceptación de los valores de la Guardia Civil.
CECLIMA	Clima social-laboral.	Ambiente generado en la unidad, departamento o equipo de trabajo. Índice de clima social.
CEIGUALDAD	Sensibilidad género. Igualdad.	Introducción de la perspectiva de género en la Institución. Igualdad de condiciones entre hombres y mujeres acceso mismo puesto bajo las mismas condiciones e iguales requisitos
CESTRUCTURA	Diseño organizativo. Plantilla. Delimitación competencias	Estructura de la Institución que establece las relaciones laborales. Distribución. Competencias funcionales.
CEDESARROLLO	Desarrollo organizativo.	Acontecimientos que propician adaptación a las situaciones actuales. Regulación de Jornadas y horarios en general.
CERUTINAS	Pautas organizativas. Procedimientos establecidos y sistemas.	Procedimientos y rutinas establecidos o nuevas competencias para mejorar la Institución. Mejora de las funciones a desempeñar por los guardias civiles, mejorando su calidad profesional y aumentando su motivación.
CERELACIONINT	Explicación de la estrategia a su personal.	Procesos dirigidos a explicar a los componentes de la Institución su Estrategia, visión, misión e innovación. Introducción de algo nuevo o modificación de lo anterior que provoque un mejor desempeño en el servicio.
CECRIMINAL	Actuaciones, denuncias e infracciones administrativas.	Procesos dirigidos a explicar, numerar y contextualizar las detenciones, denuncias e infracciones administrativas.
CEPROVEEDORES	Contratación proveedores.	Conjunto de procesos de proveedores, alineados a los valores de la Institución. Contratación pública socialmente responsable (CPSR). Orientado a los riesgos laborales, reciclaje y medio ambiente.
CEINVERSIONIDI	Inversión I+D+i. Dominios de sus sedes electrónicas.	Inversión económica en investigación y desarrollo. Gastos elaborados por su funcionamiento al desarrollar acciones innovativas, conferidas como espacios virtuales de uso exclusivo por la Institución. Dominios internet.
CEPERSONALIDI	Personal I+D+i.	Plantilla de plena dedicación a investigación y desarrollo.
CEPROYECTOSIDI	Proyectos I+D+i. Programa Marco UE. Programa Horizonte 2020.	Trabajos realizados relacionados con la innovación y el desarrollo. Proyectos generados en concordancia con el proceso innovativo con otras organizaciones o de forma independiente.
CEINFRAESTRUCTURA	Infraestructuras y material.	Mantenimiento de las instalaciones. Inversión en instalaciones e infraestructuras.
CEEQUIPOPOLICIAL	Equipamiento policial. Dotación tecnologías de producción.	Productos y herramientas adecuadas a las necesidades particulares de la Institución. Conjunto de equipos tecnológicos necesarios para el cumplimiento de un servicio.
CEINNGEST	Innovación de gestión. Innovación de modelo de Institución.	Herramientas nuevas y procedimientos compartidos en la Institución que impulsan la innovación. Transformación digital.
CECOMUNICACIONGC	Comunicación interna Relaciones asociaciones. Consejo.	Sistemas informáticos, telecomunicaciones útiles funcionamiento de la Institución. Facilidad y buena actitud en la transmisión de los conocimientos e información para la ejecución de un servicio con las personas adecuadas para ello. Atención al guardia civil.
CEMARCA	Marcas registradas. Imagen de la GC	Marca, logo y emblemas en la Institución. Referencia a los uniformes.
CELICENCIAS	Licencias forenses, subscriptores.	Procesos por el que se comparte una parte de los procesos y conocimientos de la Institución. Convenios con otras administraciones y universidades.
CESECRETO	Protección de datos.	Todos los considerados por la Institución como tales. Protección de datos (ciudadanos).
CEPATENTES	Información patentes.	Base de datos registren cantidad y uso de patentes empleadas por la Institución.
CETECNOEXT	Conocimiento actividad tecnológica competencia.	Bases de datos e información disponible sobre los avances en I+D de los competidores.
CETECNONEW	Información sobre líneas investigación y tecnología emergente.	Bases de datos de información sobre tecnología emergente que afecte a la Institución. Conocimiento posibles asociaciones con empresas para I+D.
CETECLIC	Localización tecnología sobre la que buscar licencias	Fuentes de datos sobre tecnologías útiles para ser desarrolladas en la Institución.
CEFLEXIBILIDAD	Flexibilidad y adaptabilidad.	Comportamiento favorable hacia el cambio por las situaciones derivadas del servicio o de la Institución.
CETALENTOS.	Antigüedad y fidelización de los guardias civiles.	Permanencia de los empleados basada en políticas de retención y atracción de guardias civiles que aportan valor a la Institución. Situaciones.

ELEMENTOS DIMENSIÓN CAPITAL RELACIONAL

Códigos	Unidad Muestral	Definición
CRCIU	Base ciudadanos.	Ciudadanos en general.
CRLEALCIU	Lealtad ciudadanos.	Grado de fidelidad que procesan los ciudadanos a la Institución. Primera opción en seguridad.
CRSATISFACCION	Satisfacción ciudadanos. Seguridad pública.	Grado de eficacia que el ciudadano percibe en la cumplimentación de un servicio y en general con la Institución. Felicitaciones atención al ciudadano.
CRQUEJAS	Quejas, reclamaciones y sugerencias ciudadanos.	Quejas recibidas por la prestación de un servicio y sugerencias. Atención a la ciudadanía. Oficina de Información y Atención al Ciudadano(OIAC). Puntos de Atención Especializada (PAEs).
CRPROTCIU	Procesos relación ciudadanos. Protocolos ciudadanos.	Protocolos de actuación y comportamiento con los ciudadanos. Turismo seguro. Trata de seres humanos (TSH). Mayores seguros. VdG. Menores. Víctimas de terrorismo.
CRESTADO	Relaciones Estado y UE. Accionistas e inversiones institucionales.	Grado de inversiones; recursos disponibles; presupuestos.
CRIADMINISTRACION	Relaciones Institución mercado. Relaciones con otros grupos de interés Administración.	Relaciones con otros grupos de interés de la Institución. Administración general ACCEDA; Firma digital. Partidos políticos. Firma convenios administraciones.
CRCAPITALEXTERIOR	Relaciones participación empresarial.	Capital de la Institución en otras entidades.
CRALIANZAS	Base aliados.	Alianzas con otras instituciones dentro de su área de seguridad. Relacionados con la creación de conocimiento, y su transferencia impulsando la innovación.
CRALIANZASESTABLES	Solidez alianzas. Servicios conjuntos. Estabilidad alianzas y formalización.	Formas establecidas de cooperación con policías misma área de seguridad. Innovación internacional. Nuevas formas en otros países que contribuyan al desarrollo o diversificación de la Institución o sus competencias. Misiones encomendadas por el Ministerio de Defensa.
CRALIANZASBENEFICIO	Beneficio alianzas. Resultados obtenidos alianzas.	Generación de beneficios de las alianzas establecidas. Ayuntamientos Seguridad Ciudadana y Seguridad Vial. Protección civil.
CRCONCOMPETENCIA	Conocimiento competidores.	Conocimiento otras policías en la compartición de las competencias de seguridad.
CRPRIVADA	Relaciones seguridad privada.	Grado beneficios obtenido relaciones con otros grupos de interés. Seguridad privada.
CRCERTICAL	Certificaciones y sistemas calidad.	Certificados de calidad otorgados a la Institución. Premios (SEPRONA); Igualdad.
CRREDES	Portal guardia civil exterior. Información divulgada redes.	Canales de comunicación en la Institución basado en la tecnología. Notas de prensa e información comparte Institución en Redes Sociales. Información pública.
CRADMINISTRACION	Colaboración Adm. Públicas. Cooperación para el desarrollo.	Cooperación con otras administraciones nacionales e internacionales de la Institución. Ministerios. Compras públicas innovadoras firma de Convenios con otras administraciones.
CRMEDIOS	Relaciones medios comunicación convencionales.	Exposición de la institución medios de comunicación. TVE; radio; periódicos. Medios más convencionales.
CRDEFENSAMBIENTE	Relaciones instituciones defensa medioambiental.	Grado de efectividad con otros grupos dedicados a la defensa del medioambiente.
CRVERDE	Códigos y certificaciones medio ambientales.	Procedimientos y protocolos establecidos interiorizados por la Institución en la defensa del medioambiente.
CRMERCADO	Relaciones instituciones mercado trabajo.	Relaciones institución con el mercado laboral. Contribución al tejido empresarial Oferta empleo público (OEP).
CRCODIGOCON	Código de conducta.	Nuestro código es normativo. Normas explícitas establecidas de comportamiento recogidas en el Reglamento. Código Penal Militar.
CRACSOCIAL	Acción social al ciudadano. Preocupaciones sociales	Espíritu Benemérito. Comportamiento adecuado y correcto del personal especialmente con los ciudadanos en el desempeño del servicio. Responsabilidad con la sociedad, desarrollo económico, solidaridad e integración social.
CRBUENGOBIERNO	Dirigidos a los ciudadanos. Buen gobierno.	Procesos dirigidos a la catalogación de los ciudadanos, sus riesgos y necesidades. Código buen gobierno de la AGE. Difusión de buenas prácticas. Transparencia, responsabilidad y eficacia con todos los grupos de interés. Compromiso adquirido voluntario por la Institución como forma de rendir cuentas a la sociedad a la que sirve.

Anexo II

Exemplos de cálculo de um índice de um elemento, pertencente a cada categoria.

Categoría Capital Humano

Elemento: *CHEducación*.

$$I \text{ CHEducación} = 1/14 \sum_{i=1}^{14} j = I \text{ CHEducación cuanti} + I \text{ CHEducación cualit} + I \text{ CHEducación gráfico}$$



Categoría Capital Estructural

Elemento: *CERutinas*.

$$I \text{ CERutinas} = 1/25 \sum_{i=1}^{25} j = I \text{ CERutinas cuanti} + I \text{ CERutinas cualit} + I \text{ CERutinas gráfico}$$

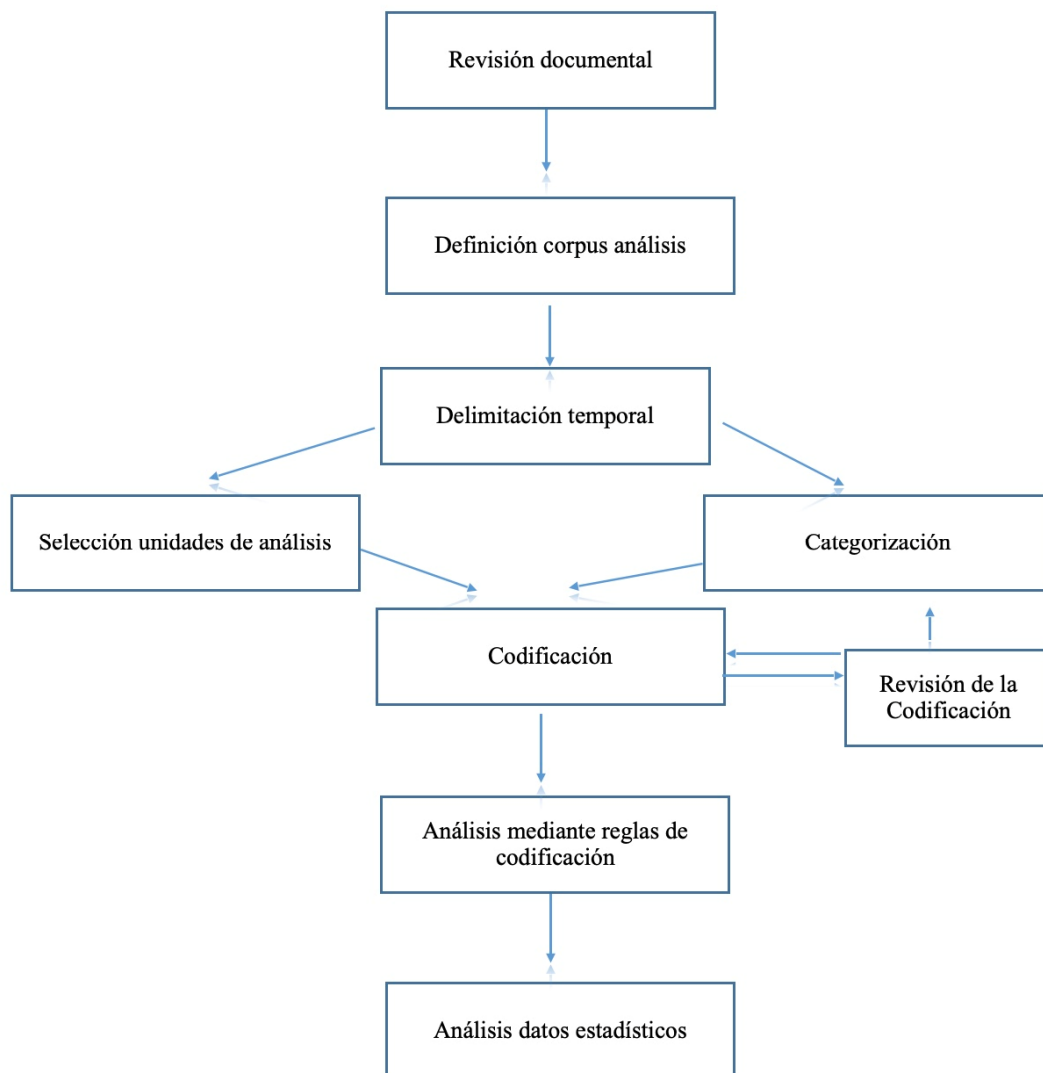
Categoría Capital Relacional

Elemento: *CRLealciu*.

$$I \text{ CRLealciu} = 1/23 \sum_{i=1}^{23} j = I \text{ CRLealciu cuanti} + I \text{ CRLealciu cualit} + I \text{ CRLealciu gráfico}$$

Anexo III

Fases desarrolladas na análise de conteúdo





III.- RESENHAS DE JURISPRUDÊNCIA



Revisão da jurisprudência

REVISÃO DE JURISPRUDÊNCIA 2ª SECÇÃO DO SUPREMO TRIBUNAL

Tradução para o português com ajuda de IA (DeepL)

Javier Ignacio Reyes López
Magistrado do 46º Tribunal de Instrução de Madrid
Diploma de Estudos Avançados (DEA)
ji.reyes@poderjudicial.es

Recebido a 06/06/2025
Aceite em 06/06/2025
Publicado em 27/06/2025

Citação recomendada: Reyes, J. I. (2025). Reseña de jurisprudencia Sala 2ª Tribunal Supremo. *Revista Logos Guardia Civil*, 3(2), p.p. 295-320.

Licença: Este artigo é publicado sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Depósito legal: M-3619-2023

NIPO em linha: 126-23-019-8

ISSN em linha: 2952-394X

REVISTA DE JURISPRUDÊNCIA 2ª SECÇÃO SUPREMO TRIBUNAL

Resumo: STS 350/2025, de 10 de abril. Conceito de interessado numa busca domiciliária. 2 - STS 358/2025, de 10 de abril de 2025. Notícia criminal transferida para Espanha por uma autoridade judicial estrangeira e continuação da investigação no nosso país com novas investigações. 3.- STS 324/2025, de 07 de abril de 2025. Conservação de dados de comunicações. 4.- STS 294/2025, de 28 de março de 2025. Princípio da insignificância e da toxicidade nos crimes contra a saúde pública. 5 - STS 8/2025, Secção Penal 3ª, de 2 de abril de 2025. Delito de destruição com fins terroristas. 6 - STS 308/2025, de 2 de abril de 2025. Investigação policial em Espanha decorrente do conhecimento de um IEP emitido pelas autoridades judiciais de outro país por outra infração penal. Presença de detidos numa busca domiciliária. 7.- STS 295/2025, de 28 de março de 2025. Crime de assédio, "stalking". 8 - STS 284/2025, de 27 de março. Abuso sexual de uma pessoa de 17 anos com inteligência limítrofe. Danos morais.

1 - STS 350/2025, de 10 de abril. Conceito de interessado numa procura de casa .¹

Antecedentes factuais.

O Juzgado de Instrucción nº 5 de Marbella abriu o processo abreviado nº 104/2018 por um suposto crime contra a saúde pública contra Noelia, entre outros, que, uma vez concluído, foi remetido para julgamento à 1ª Secção do Tribunal Provincial de Málaga. O processo abreviado nº 1004/2019 foi aberto em 17 de maio de 2021, tendo o Tribunal proferido a sentença nº 233/2021, na qual declarou como provado que, "...Tendo em conta as provas, declara-se expressa e categoricamente provado que o Grupo de Crime Urbano da Delegacia de Policía CNP Marbella realizou uma operação de vigilância para detetar a venda de substâncias na área xx de Marbella, que está localizada entre o Parque Industrial Ermita e o Boulevard da Avenida José Manuel Valles e ao lado de uma escola, um ponto frequente e conhecido pelo seu conflito e por ser um ponto de venda e consumo de drogas. Tomaram conhecimento da existência do clã dos "Chatos" dedicado à venda de substâncias estupefacientes através de imóveis situados neste bairro de lata, pois tinham conhecimento de que os seus residentes poderiam estar envolvidos na venda de substâncias estupefacientes, uma vez que havia um fluxo diário de pessoas que faziam pequenas visitas. Como resultado da vigilância, observação exaustiva, interceção e apreensão sucessiva, através de denúncias de estupefacientes por parte de pessoas que vinham especificamente comprar nas casas investigadas, são recolhidos os seguintes relatórios... e posteriormente, com base no pedido policial, pelo Tribunal de Instrução n.º 5 de Marbella, foi emitido um despacho em 4 de junho de 2018 autorizando a entrada e busca, entre outros, nas várias casas em que foram apreendidas substâncias estupefacientes e os investigados foram detidos..."

¹ STS 350/2025, Secção Penal 1 de 10 de abril. Publicado no sítio Web do Centro de Documentação Judiciária, CENDOJ, (ROJ: STS 1701/2025 - ECLI:ES:TS:2025:1701), recurso n.º 7569/2022. Relator: Eduardo de Porres Ortiz de Urbina.

Base jurídica.

Está a ser interposto um recurso de cassação no Supremo Tribunal contra a sentença número 197/2022, de 14 de julho de 2022, proferida pela Divisão Civil e Criminal do Tribunal Superior de Justiça da Andaluzia, Ceuta e Melilla, que rejeitou o recurso interposto contra sentença número 233/2021, de 17/05/2021, da 1ª Secção do Tribunal Provincial de Málaga, condenando por um crime contra a saúde pública. Das quatro pessoas condenadas, apenas uma interpôs recurso.

O primeiro fundamento de recurso alega que o acórdão recorrido violou o direito à privacidade no domicílio do artigo 18.2 CE e o direito a um julgamento com todas as garantias reconhecidas no artigo 24.2 da Constituição.

Alega que se encontrava detida no momento das buscas domiciliárias e que só podia estar presente numa delas (a casa de onde estava a sair quando foi detida) e não nas outras casas, em relação às quais lhe foi atribuída uma ligação criminosa.

A defesa entende que a presença do interessado é um requisito inescusável para a realização de uma busca domiciliária, nos termos do art. 569.º da LECrim, sendo nulas as buscas domiciliárias que não cumpram este requisito quando o interessado esteja detido e não exista outro motivo que o impossibilite, pelo que não é admissível como prova para a acusação, nem são admissíveis como prova para a acusação as declarações dos agentes policiais que intervieram nas buscas.

Considera que, no caso vertente, a nulidade da busca conduz à impossibilidade de afirmar juridicamente a descoberta da substância e dos objectos de cuja posse decorre a condenação pelos crimes contra a saúde pública e de posse ilegal de armas, e que esta apreensão não pode ser sancionada através do testemunho dos agentes presentes na busca, uma vez que os respectivos testemunhos estão diretamente ligados à ação ilegal.

Esta questão foi levantada no recurso anterior e os argumentos para a sua rejeição são os nossos.

Neste procedimento, foram realizadas sete buscas simultâneas e, em cinco delas, a busca foi efectuada na presença dos interessados em cada uma das propriedades, exceto em duas delas, em que ninguém foi encontrado e a busca foi realizada, como nas outras, sob a supervisão do Consultor Jurídico para a Administração da Justiça.

A recorrente estava presente no momento da busca na sua casa e não podia estar presente nas outras casas, porque as buscas foram simultâneas e porque, em princípio, não era residente nas outras casas e não foi localizada nem detida. A sua detenção teve lugar precisamente no momento da busca.

O artigo 569.º da LECrim estipula que a busca numa casa particular será efectuada na presença do interessado ou da pessoa que legitimamente o represente. A jurisprudência desta Câmara tem sido hesitante quando se trata de especificar o que deve ser entendido por "parte interessada", uma vez que em alguns acórdãos foi considerado que se trata da pessoa que possui a casa afetada, como titular do direito à privacidade afetado pela interferência (SSTS. 18.7.98, 16.7.2004 e 3.4.2009), enquanto outros acórdãos consideraram que a pessoa que é objeto da investigação policial tem esse carácter, na

medida em que tem um interesse direto no resultado da busca devido às repercussões processuais e penais que podem derivar do seu desenvolvimento (SSTS 27.10.99, 30.1.2001 e 26.9.2006). Esta última posição é a maioritária, pelo que a presença do interessado é exigida no processo, mesmo que não seja o proprietário da casa, no caso de o interessado ser detido. No STS 771/2010, de 23 de setembro, seguido por muitos outros, afirmava-se que a jurisprudência é certamente uniforme no sentido de exigir a presença do interessado - a pessoa sob investigação - na busca nos casos em que é detido e mesmo no caso de ser diferente do proprietário da casa ou de este estar presente ou se recusar a estar presente na busca. Essa presença, se possível, é exigida devido aos requisitos de contraditório que devem rodear qualquer procedimento probatório e, mais ainda, devido às características das buscas domiciliárias em que a ausência de contraditório no próprio ato da busca não pode ser cumprida devido à atividade contraditória que torna possível o debate do julgamento oral. Por isso, se o interessado estiver detido, a sua presença na busca é obrigatória, não se aplicando as exceções previstas nos n.ºs 2 e 3 do art. 569.º da LECrim (SSTS. 833/97 de 20.6, 40/99 de 19.1, 163/2000 de 11.2, 1944/2002 de 9.4.2003).

No entanto, há casos em que essa presença não é possível e há várias circunstâncias que podem impossibilitar essa presença: que a pessoa sob investigação não possa ser localizada, que não queira comparecer se não estiver detida e que esteja fisicamente impossibilitada de o fazer, como acontece nos casos de buscas simultâneas. Neste último caso, tal foi reconhecido por esta Câmara em numerosos acórdãos, como os SSTS 947/2006, de 26 de setembro, 771/2010, de 23 de setembro, e 199/2011, de 30 de março.

No caso em apreço, a recorrente estava presente na busca ao seu domicílio e não estava presente nas outras buscas, porque estas foram efectuadas simultaneamente.

Por conseguinte, o fundamento é julgado improcedente e o acórdão recorrido é mantido na sua totalidade.

Conclusões.

Em poucas ocasiões o CS manteve uma linha tão uniforme sobre quem deve ser considerado interessado numa entrada e busca, sendo a pessoa que, independentemente do título formal detido em relação à casa, pode ser legalmente afetada pelo seu resultado no crime em investigação. Descrevem-se ainda os problemas práticos entre buscas sucessivas e simultâneas, de modo a que o interessado possa assistir a este procedimento, salvo se, por razões excepcionais ou de força maior, tal não for viável.

2 - STS 358/2025, de 10 de abril de 2025. Notícia-crime transferida para Espanha por uma autoridade judiciária estrangeira e continuação da investigação no nosso país com novas investigações policiais .²

Antecedentes factuais

No processo n.º 33/2021 (decorrente do PA 25/2021 do Juzgado de Instrucción n.º 3 de Talavera), seguido perante a Audiencia Provincial de Toledo, Sección 1ª, em 5 de maio de 2022, Evelio foi condenado como autor de um crime contra a saúde pública por tráfico de estupefacientes, que contém os seguintes factos provados: "...Na sequência de uma comunicação enviada pelo Ministério Público em Portugal, soube-se que poderia existir um grupo organizado que, a partir da América do Sul, era responsável pelo envio de cocaína para a Europa, pelo menos para Espanha e Portugal, e que para o efeito utilizava embarcações que faziam escala no porto do Porto. E que, a partir dessa cidade, pelo menos em parte, a cocaína era transportada por camião até à cidade de Talavera La Nueva, onde era descarregada num armazém industrial com a marca Puertas Artevi. Na sequência desta informação, o Udyco iniciou uma investigação que resultou na verificação da veracidade da informação relativa à chegada de camiões ao armazém, pelo que iniciou uma série de vigilância e monitorização que lhes permitiu descobrir que o armazém foi alugado pelo arguido Evelio, nascido em 1984, sem antecedentes criminais, que também alugou um armazém na localidade de Ventas de Retamosa e um armazém, com o número, propriedade da empresa Blue Space, de Leganés. Por ordem de 22 de dezembro de 2020, o Tribunal de Primeira Instância e Investigação Preliminar número três de Talavera autorizou a entrada e a busca nos armazéns acima mencionados e na sala de armazenamento. Na sala de armazenamento foram encontrados sete pacotes rectangulares, contendo uma substância branca, à qual foi aplicado o reagente apropriado, que deu positivo para cocaína. Após a correspondente análise, verificou-se tratar-se de cocaína, com um peso total de seis mil e noventa e seis gramas e uma riqueza média de 77,88%, e cujo valor no mercado ilícito ascenderia à quantia de duzentos e trinta e oito mil trezentos e sessenta e nove e trinta e um euros, que o arguido possuía para distribuição por terceiros. Não ficou provado que os outros arguidos, Gaspar, nascido em 2002, sem antecedentes criminais, e Jacinta, nascida em 1991, que foi condenada na sentença de 16 de junho de 2020 por um crime contra a saúde pública, estivessem relacionados com a substância apreendida...".

Base jurídica

O recorrente pede a anulação do despacho que ordenou as escutas telefónicas do recorrido e do despacho de 29 de julho de 2020, pelo qual foi prorrogado, bem como novas escutas, pedidos que foram apresentados pela primeira vez como questão prévia ao início do julgamento oral e que já foram rejeitados pelo tribunal de primeira instância com argumentos adequados.

O fundamento, como dissemos, coincide com o invocado no recurso, com a única diferença de que transcreve um parágrafo do STSJ, mas com o qual não discute, repetindo

² STS 358/2025, de 10 de abril de 2025, publicado na página web da CGPJ pelo Centro de Documentação Judicial, CENDOJ, (ROJ: STS 1628/2025 - ECLI:ES:TS:2025:1628). recurso: 8375/2022. Interveniente: Sr. Ángel Luis Hurtado Adrián.

que a nulidade dos referidos despachos se baseia na falta de fundamentação e justificação, uma vez que carecem de finalidade e ultrapassam as disposições contidas no quadro de colaboração entre as autoridades espanholas e as autoridades portuguesas, e a irregularidade imputada a esses despachos deve-se ao facto de as pessoas onde a droga seria armazenada e escondida já terem sido identificadas através da vigilância policial efectuada nos dias 14, 15, 17 e 19 de maio, pelo que, no entender do recorrente, não existe fundamento nem base legal para o pedido da polícia de autorização de escutas telefónicas 25 dias depois.

Alega-se que o objeto da vigilância era a chegada de Portugal de um camião com um carregamento para ser depositado no armazém no dia 14 de maio de 2020, e que, estando a chegada e a descarga sob vigilância, é lógico que a intervenção policial deveria ter sido feita nesse dia ou nos dias seguintes, e que se não é feita, é porque não há certeza de que a droga tenha chegado ali. Se assim for e 25 dias depois a escuta telefónica for acordada, o signatário do recurso considera que se trata de uma investigação prospetiva, porque nessa altura não há indícios de que esteja a ser cometido ou venha a ser cometido qualquer crime, e volta a repetir que, quando o despacho em causa foi emitido, não existia qualquer "razão plausível" ou "forte presunção" que justificasse essa intervenção, e fá-lo sem aduzir qualquer argumento às considerações que, para rejeitar tal abordagem, o acórdão de primeira instância e, depois, o acórdão de recurso lhe fizeram, quando reitera, uma vez mais, uma alegação com consequências tão traumáticas como a nulidade por considerar a investigação prospetiva, a que deveria ter dado bastante mais extensão depois de a ter rejeitado em duas ocasiões anteriores.

A abordagem do recorrente assenta na ligação entre a ação policial que teve lugar a partir do dia 14, na sequência de informações recebidas das autoridades portuguesas, e a investigação objeto dos presentes autos, o que resulta da leitura dos factos provados, que remete para a comunicação enviada pelo Ministério Público português, que revelou a existência de um grupo organizado responsável pelo envio de cocaína para a Europa, que chegava pelo porto do Porto e daí era transferida, pelo menos em parte, para o edifício industrial com a etiqueta Puertas Artevi, na localidade de Talavera de la Reina, arrendado por Evelio, em torno do qual estava a decorrer uma investigação em Portugal, que levou à emissão de uma Ordem de Investigação Europeia pelo Ministério Público do Porto, solicitando determinadas diligências no nosso país, e que, conforme consta do despacho de 22 de dezembro de 2020, por despacho de 29 de junho de 2020, foi acordado reconhecer e executar. Entre as medidas tomadas, conta-se a interceção de alguns telefones, incluindo o do referido Evelio, que foi prorrogada por despacho de 29 de julho de 2020 e anulada por despacho de 18 de setembro de 2020, investigação portuguesa na qual não há registo de que tenha sido constituído arguido.

As investigações policiais prosseguiram no nosso país, através do Udyco, por meio de vigilância e monitorização, tendo-se apurado que, entre outras coisas, o referido Evelio cumpria medidas de segurança, conforme consta do despacho, indiciadoras de uma presumível atividade criminosa relacionada com um crime de tráfico de estupefacientes, diferente e posterior àquela que poderia ser objeto de investigação em Portugal, uma vez que, como explica o acórdão do tribunal de primeira instância, "não há indícios de que os arguidos tenham sido processados no país vizinho, pelo que a investigação não poderia limitar-se apenas à identificação dos eventuais autores que em Espanha praticaram os factos objeto do processo penal em Portugal".

Em todo o caso, as informações iniciais, ainda que provenientes de Portugal, forneceram elementos que justificaram a adoção das medidas tomadas pelo juiz de instrução, incluindo a que limita os direitos fundamentais, como as escutas telefónicas acordadas, que, por isso, não podem ser consideradas como tendo sido prestadas no decurso de uma investigação prospetiva, mas que, ao mesmo tempo, foram úteis para investigar a presumível atividade criminosa que estava a ser cometida em Espanha, e sustentar o contrário, como argumenta o M.F., é "um raciocínio difícil de sustentar, pois o recorrente parece pretender que na investigação de um crime de que tem conhecimento prévio, é necessário renunciar a investigar a existência de outros possíveis participantes num crime, é "um raciocínio difícil de manter, pois o recorrente parece pretender que, na investigação de um crime de que tem conhecimento prévio, é necessário renunciar a investigar a existência de outros possíveis participantes num crime tão grave como o do caso em apreço".

Isso mesmo é explicado no acórdão recorrido, que expõe as razões pelas quais os factos investigados em Portugal devem ser dissociados dos que seriam investigados no nosso país, ainda que em ambos os casos estivessem relacionados com crimes de tráfico de estupefacientes, porque a rutura entre ambos é evidente, devendo cada um, fazendo nossas as palavras que acabamos de transcrever do M.F., dar lugar a uma investigação própria. O acórdão recorrido também explica este aspeto, que diferencia as investigações portuguesa e espanhola, quando diz que "a investigação não tinha de se limitar apenas à identificação das pessoas e do local onde escondiam droga, pois não se tratava de colaborar com as autoridades portuguesas relativamente a factos que eram objeto de processo-crime em Portugal, nem há registo de processos-crime contra os arguidos nesse país, mas sim de informações enviadas pelo Ministério Público português à polícia espanhola sobre factos dos quais se poderia deduzir a eventual prática de um crime em Espanha, incorporando dados objectivos indicativos de atividade criminosa no nosso país, como a chegada de um navio, o carregamento de bobinas, as empresas transportadoras e, sobretudo, o destino em Espanha do material carregado em Portugal".

Em suma, dispondo o juiz de instrução de indícios suficientemente plausíveis para aferir da presumível prática de um crime de tráfico de estupefacientes no nosso país, ainda que fornecidos por informações provenientes de Portugal, não se pode falar de uma investigação prospetiva, porque foram essas informações que lhe forneceram esses elementos, em função dos quais adoptou as medidas de investigação que considerou adequadas, incluindo a escuta telefónica de um dos presumíveis implicados, o que justificou suficientemente no seu despacho de 29 de junho de 2020 e também no despacho de prorrogação de 29 de julho de 2020.

O recurso é julgado improcedente na sua totalidade e a condenação do recorrente é confirmada.

Conclusões.

O CF avalia o alcance de uma OEI formalmente enviada pela autoridade judiciária portuguesa à autoridade judiciária nacional, como instrumento de cooperação que implicava algumas medidas restritivas dos direitos fundamentais. Quando essa linha de investigação não prosperou e não foi concluída, nem foi seguido um processo penal independente em Portugal sobre os mesmos factos, a Polícia Judiciária espanhola acrescentou a essa informação novos dados sobre as pessoas sob investigação e possíveis

actos criminosos cometidos em Espanha, e iniciou um procedimento que, com base no primeiro, permitiu dismantlar um grupo criminoso dedicado à prática de crimes graves.

3.- STS 324/2025, Secção Penal 1 de 07 de abril de 2025. Conservação de dados de comunicações . 3

Antecedentes factuais

O Tribunal Provincial de Barcelona, 7ª Secção, proferiu a sentença nº 173/2023 de 3 de março, decorrente do processo sumário nº 1/2021 do Tribunal de Instrução nº 1 de Sant Boi de Llobregat, seguido de um crime contra a saúde pública, que contém, entre outros, os seguintes factos provados: "...são factos provados, e assim se declara, que desde pelo menos no mês de agosto de 2018 os arguidos Jenaro, Humberto, Fermín, Lucas e Emiliano formaram um quadro pessoal, material, empresarial e logístico colocado ao serviço de um plano comum que consistia em obter cocaína escondida num contentor do Brasil que chegaria ao porto de Barcelona em meados de dezembro, para proceder à sua distribuição nesta última província. Jenaro estava no topo da rede, dando-lhe cobertura financeira e contactos para obter a droga; Humberto era responsável pela gestão e coordenação. Fermín era o responsável pela estrutura empresarial e de negócios capaz de se apoderar do carregamento fazendo-o passar por uma compra e venda legal de folhas de papel Din-A4, Lucas era o responsável pela logística, especialmente pela organização do transporte da substância, de que Emiliano se encarregaria, delegando-o em terceiros.

Na execução deste plano criminoso, a empresa Campderros Salvans S.L., adquiriu, através de Fermín, 1.600 caixas de folhas de papel DIN-A4 da empresa Precisión Comercio Internacional LTDA, com sede em Pinheiro-Maceió (Brasil), cuja chegada ao Porto de Barcelona estava prevista para dezembro de 2018; mercadorias que foram distribuídas em dois contentores com 800 caixas de folhas DIN-A4 cada, contentores numerados APZU3035695 e APZU3807079 fretados a bordo do navio da companhia de navegação CMA-CGM RIO GRANDE, navegando do Porto de Itaguaí (Rio de Janeiro-Brasil) para o Porto de Barcelona, em 21 de novembro de 2018...." O relato dos factos provados continua dizendo que, "...Às 13:40 horas da data acima mencionada, durante o trabalho de carregamento e redistribuição dos pacotes de fólhos no camião conduzido por Herminio, caiu acidentalmente da empilhadeira mecânica empregada por um dos trabalhadores da Campderros Salvans S.L., Nemesio, uma caixa de papel de alumínio que saía do contentor com o número APZU 3035695, a qual, ao ser partida, revelou vários pacotes rectangulares que vieram a conter a referida substância estupefaciente. Solicitada a presença policial, chegou ao local uma equipa de agentes dos Mossos d'Esquadra que, depois de inspecionar devidamente todas as caixas de papel de alumínio, localizou no seu interior 1.410 embalagens rectangulares com as seguintes características identificativas..."

Base jurídica

Num longo acórdão, o CS passa em revista as numerosas contestações feitas pelos advogados de defesa dos arguidos na tentativa de desmontar a justeza das condenações, salientando mesmo que um dos recorrentes critica o juiz de instrução por não ter

³ STS 324/2025, Secção Penal 1ª de 07 de abril de 2025, publicada na página web da CGPJ pelo Centro de Documentação Judicial, CENDOJ, (ROJ: STS 1487/2025 - ECLI:ES:TS:2025:1487). Recurso: 10408/2024. Interveniente: Manuel Marchena Gómez.

acrescentado à ingerência que as escutas telefónicas representam, outras medidas que reforçam a ingerência do Estado no círculo de exclusão definido pelo direito à privacidade. Não faz sentido invocar a nulidade de um ato judicial de ingerência na vida privada de um suspeito censurando o juiz por não ter autorizado restrições ainda mais severas do que as consideradas necessárias e proporcionais.

Raramente, como no presente caso, qualquer queixa relativa a uma possível investigação prospetiva ou contrária aos princípios da proporcionalidade, da necessidade ou da excecionalidade - artigo 588º-A - deve necessariamente ser rejeitada.

A partir do momento em que a droga foi descoberta por acaso, devido a um acidente durante o descarregamento, o trabalho das Forças e do Corpo de Segurança do Estado, com o objetivo de descobrir quem tinha adquirido este carregamento extraordinário de cocaína para distribuição clandestina, foi plenamente justificado. Este trabalho, além disso, estava sujeito ao controlo restritivo do juiz de instrução n.º 1 de Sant Boi de Llobregat e à intervenção fiscalizadora do Ministério Público (art. 306.º da LECrim).

Passamos agora à contestação da conservação dos dados de comunicação.

O fundamento incorpora uma alegação relativa ao pedido dos Mossos aos operadores telefónicos para conservarem os dados para além do prazo de 1 ano imposto pela Lei 25/2007, de 18 de outubro de 2007, relativa à conservação de dados, com uma referência marginal ao acórdão do Tribunal de Justiça da União Europeia, de 8 de abril de 2014, que declarou a nulidade da Diretiva 2006/24/CE.

A defesa alega que o pedido de conservação destes dados - que não foi formalmente integrado no processo - não foi previamente autorizado pelo juiz de instrução.

O acórdão recorrido critica a recorrente por pretender esta nulidade através de uma alegação genérica em que não se indica quais as ordens ou linhas interceptadas que seriam afectadas". E considera que a autorização judicial está implícita nas decisões de habilitação que implicam, pela sua própria natureza, a necessidade de conservar os dados ligados a esses processos de comunicação.

Em todo o caso, a Câmara considera que essa autorização judicial para obrigar os operadores ou qualquer outra pessoa singular ou colectiva a conservar os dados não é obrigatória.

Isto pode ser deduzido das disposições do art. 5 da Lei 25/2007, de 18 de outubro, sobre a conservação de dados relativos a comunicações electrónicas e redes públicas de comunicações. E o mesmo se deduz do art. 588 *octies* da LECrim, que regula a ordem prévia de conservação de dados como medida de segurança.

A primeira destas disposições é dirigida aos operadores que prestem serviços de comunicações electrónicas acessíveis ao público ou explorem redes públicas de comunicações, nos termos estabelecidos na Lei n.º 32/2003, de 3 de novembro, Lei Geral das Telecomunicações", critério reiterado em art. 1.º da atual Lei n.º 9/2014, de 9 de maio, Lei Geral das Telecomunicações.

A segunda - art. 588 octies da LECrim - incorpora o mesmo dever de segurança e preservação dos dados quando o depositário é uma pessoa singular ou colectiva e exclui expressamente a necessidade de autorização judicial: "o Ministério Público ou a Polícia Judiciária podem exigir a qualquer pessoa singular ou colectiva que conserve e proteja dados ou informações específicos incluídos num sistema de armazenamento informático à sua disposição até que seja obtida a correspondente autorização judicial para a sua transferência, de acordo com o disposto nos artigos anteriores".

Assim, tanto o Ministério Público como as Forças e Corpos de Segurança do Estado estão habilitados a emitir, sem necessidade de autorização judicial, essa ordem de conservação, que, logicamente, só faz sentido no âmbito de uma investigação em que seja previsível a necessidade posterior de incorporar esses dados no processo penal instaurado.

A não exigência de autorização judicial resulta não só da redação deste preceito, mas também da exposição de motivos da LO 13/2015, de 5 de outubro, que introduziu o art. 588º octies, ao referir que, finalmente, e no que respeita aos processos de investigação tecnológica, a reforma contempla como medida de segurança a ordem de conservação de dados, que tem por finalidade garantir a conservação de dados concretos e informações de todo o tipo que se encontrem armazenados num sistema informático até à obtenção da correspondente autorização judicial.

Conclusões

Esta STS distingue claramente entre uma medida de conservação de dados e outras medidas tecnológicas, distinguindo entre quando é necessária uma autorização judicial e quando o FCSE pode atuar diretamente. As medidas tecnológicas previstas no artigo 588.º-A e seguintes da LECrim, que em alguns casos não foram actualizadas, como a utilização de drones, a utilização de IA...

4.- STS 294/2025, de 28 de março de 2025. Âmbito de aplicação do princípio da insignificância e da toxicidade nos crimes contra a saúde pública .4

Antecedentes factuais.

O Tribunal de Instrução nº 11 de Palma de Maiorca, abriu o processo preliminar nº 649/2020, uma vez concluído foi enviado ao Tribunal Penal nº 2 de Palma de Maiorca, para julgamento no processo abreviado nº 11/2022, que ditou a Sentença nº 111/2022, datada de 28 de março de 2022, que contém os seguintes factos comprovados: "...ÚNICO. Fica provado e declarado que o arguido Lázaro, maior de idade, sem antecedentes criminais e privado de liberdade por esta causa no dia 9 de julho de 2020, por volta das 00:15 horas do dia 9 de julho de 2020, por volta das 00:15 horas do dia 9 de julho de 2020:15 horas do dia 9 de julho de 2020, encontrava-se na Calle General García Ruiz em Magalluf, contactando um turista britânico a quem ofereceu cocaína em troca de 50€, entregando-lhe um invólucro com a referida substância, recebendo a quantia de 50€, facto que foi observado por uma força policial local de Calviá que parou o seu veículo e se dirigiu ao local onde o sujeito britânico tinha ido juntamente com um amigo,

⁴ STS 294/2025, Secção Penal 1ª de 28 de março de 2025, publicado no site da CGPJ, Centro de Documentação Judicial, CENDOJ, (ROJ: STS 1335/2025 - ECLI:ES:TS:2025:1335), recurso: 6755/2022. Intervém a Exma. Sra. Susana Polo García.

Encontraram-nos sentados a cheirar a substância e disseram-lhes que tinham acabado de comprar cocaína a um jovem de cor e que tinham pago 50€, tentando esconder com os pés a cocaína que tinha ficado no invólucro. Seguiram então em direção oposta e procederam à interceção de Lázaro, interceptando 50€ na sua carteira e mais 50€ no tecido das suas calças onde usava um cordão como cinto. A substância que permaneceu no invólucro, depois de analisada, revelou-se ser cocaína com um grau de pureza de 19,15% e um valor de venda ao público de 4,83 euros...".

A decisão do Tribunal Penal foi objeto de recurso para o Tribunal Provincial, que negou provimento ao recurso. O CS deu provimento ao recurso e proferiu uma sentença de absolvição.

Base jurídica.

A jurisprudência admite a atipicidade da conduta de tráfico quando, pela sua absoluta insignificância, a substância deixa de constituir uma droga tóxica ou estupefaciente pelos seus efeitos, para passar a ser um produto inócuo pela sua precária toxicidade (SSTS 527/1998, de 15 de abril; 985/1998, de 20 de julho; 789/99, de 14 de abril; 1453/2001, de 16 de julho; 1081/2003, de 21 de julho; e 14/2005, de 12 de fevereiro). O princípio da insignificância impõe a impunidade quando a quantidade de droga é tão pequena que é incapaz de produzir qualquer efeito nocivo para a saúde. Não existe ilicitude material por ausência de risco real para o direito protegido (SSTS 1441/2000, de 22 de setembro; 1889/2000, de 11 de dezembro; 1591/2001, de 10 de dezembro; 1439/2001, de 18 de julho; e 216/2002, de 11 de maio).

Por outro lado, é de assinalar que a nossa jurisprudência mais recente qualificou a utilização do termo "insignificância", preferindo falar de "toxicidade". O que não é abrangido pelo âmbito de aplicação da infração é a transmissão de substâncias que, devido à sua falta de nocividade, não implicariam um risco.

Esta doutrina deve ser aplicada de forma excecional e restritiva, mas com segurança. Neste contexto, esta Câmara continua a trabalhar com os critérios estabelecidos na sessão plenária de 24 de janeiro de 2003. Tal é confirmado por numerosos precedentes (SSTS 936/2007, de 21 de novembro; 1110/2007, de 19 de dezembro; 183/2008, de 29 de abril; e 1168/2009, de 16 de novembro) (ver STS 587/2017, de 20 de julho).

Ora, no que diz respeito ao conceito de mínimo psicoativo, e às suas repercussões penais no elemento subjetivo do delito, STS 1982/2002, de 28 de janeiro de 2004, diz-nos que os mínimos psicoactivos são aqueles parâmetros oferecidos por um organismo oficial de reconhecida solvência científica, como o Instituto Nacional de Toxicologia, que supõem um grau de afetação do sistema nervoso central, determinando uma série de efeitos sobre a saúde das pessoas, Trata-se, evidentemente, de drogas nocivas, uma vez que contêm um nível mínimo de toxicidade e, além disso, produzem uma componente de dependência, o que significa que a falta de consumo leva à compulsão. São, portanto, drogas que causam danos à saúde pública, entendida como a saúde dos indivíduos membros da comunidade, e cujas penas são concebidas pelo legislador penal, consoante os danos sejam ou não graves. Estes mínimos pressupõem que a quantidade transmitida é algum tipo de substância estupefaciente, tóxica ou psicotrópica incluída nas convenções internacionais sobre a matéria, através das listas para o efeito. Cumprem, portanto, a

natureza objetiva da infração e afectam tanto a ilicitude formal como a material. Tais mínimos têm sido oferecidos pelo relatório do Instituto Nacional de Toxicologia, e dentro das margens permitidas por tal perícia, podem ser interpretados, sem que tal implique necessariamente qualquer automatismo judicial (STS 580/2017, de 20 de julho).

Por outras palavras, qualquer substância estupefaciente que ultrapasse a dose psicoactiva mínima gera o dano para a saúde que a norma típica sanciona e, consequentemente, se for gravemente prejudicial para a saúde devido à sua natureza e classificação, continua a sê-lo, independentemente da quantidade e pureza (ou grau de adulteração, se preferir), uma vez ultrapassada a dose psicoactiva mínima (STS 723/2017, 7 de novembro).

Em todo o caso, porque sobre esta matéria devemos recordar a nossa doutrina jurisprudencial, que teve origem na Sessão Plenária Não Jurisdicional de 24 de janeiro de 2003 que, em relação à cocaína, estabeleceu que o seu princípio ativo actua a partir de 50 miligramas (0,05 gramas); Este critério foi aceite pela Câmara e retomado na Sessão Plenária Não Jurisdicional de 3 de fevereiro de 2005, na qual se acordou "continuar a manter o critério do Instituto Nacional de Toxicologia quanto às doses mínimas psicoactivas, até que se produza uma reforma legal ou se adopte outro critério ou alternativa".

Com efeito, como salienta o recorrente, o relato factual não inclui a quantidade de cocaína apreendida; além disso, de acordo com o relatório do Departamento de Saúde da Delegação do Governo das Ilhas Baleares, a substância apreendida pela polícia era de 0,093 gramas de cocaína. Por conseguinte, se, como se afirma nos factos provados, a pureza é de 19,15%, temos um total de 0,017 gramas de cocaína líquida, ou seja, 17 miligramas, o que é claramente inferior aos 50 miligramas acima dos quais existe um risco para a saúde pública.

Se é certo que o relato factual relata, de forma incompleta, um acontecimento que poderia constituir, no seu conjunto, um ato de tráfico, a verdade é que, no final, apenas se declara provada a ocupação do alegado comprador - não identificado, embora a polícia afirme ter falado com ele - de uma quantidade infinitesimal de droga, 0,093 gramas, com uma pureza de 19,15%, Encontramo-nos, pois, com um total de 0,017 gramas de cocaína líquida -17 miligramas-, quantidade inferior à dose mínima psicoactiva, sem que se considere expressamente acreditada a ocupação de outras substâncias estupefacientes pelo arguido, pelo que não se pode razoavelmente inferir, desta quantidade mínima, que estivesse envolvido no tráfico e, sobretudo, deve considerar-se que carece de relevância penal pela sua inocuidade para a saúde pública.

Conclusões.

Apesar da clareza do relato dos factos provados, um ato de tráfico de droga a retalho em que se detalha o papel do comprador e do vendedor, este STS não acrescenta nada de novo à linha de jurisprudência já seguida há anos e que se mantém inalterada, sobre o princípio da insignificância, agora alargado com a qualificadora da toxicidade, quando se trata de aplicar o critério do INTCF sobre as doses psicoactivas mínimas para avaliar o carácter criminoso da infração.

5.- RAS 8/2025 de 2 de abril de 2025. Infração penal de actos de destruição relacionados com o terrorismo . 5

Antecedentes factuais.

O presente processo judicial foi iniciado em virtude de uma comunicação via fax da Secretaria de Estado do Interior, TEPOL, informando sobre a explosão de um engenho explosivo controlado no Aeroporto "El Altet" de Alicante, tendo o Tribunal Central de Instrução n.º 2 de Madrid emitido uma ordem de início do processo preliminar em 31 de julho de 1995 e, após a investigação correspondente, foi emitida uma acusação em 19 de maio de 2010 contra Melisa pelos crimes de destruição terrorista em grau de frustração.

Base jurídica.

Esta sentença do Tribunal Superior Nacional indica que no acervo probatório do processo encontramos, em primeiro lugar, um relatório do Quartel da Guarda Civil de Guipúzcoa, de 10 de maio de 2001, a fls. 294 e ss. do volume I do processo, que informa o Tribunal Central de Instrução Prévia de que a arguida, noutros processos (26/01), também reconhece expressamente ter colocado o engenho no Aeroporto de Alicante, em que se informa o Tribunal Central de Instrução de que a arguida, noutros processos (26/01) também do referido Comando, reconhece expressamente que colocou o engenho no Aeroporto de Alicante juntamente com outra pessoa (que não está a ser julgada) dentro de um saco e dentro de um cesto de papéis. Estas afirmações constam da sua segunda declaração prestada na Guardia Civil em 31 de março de 2001 (fls. 163 do volume I do processo), na qual também refere que foi nesse mesmo dia que colocou outro engenho no posto de turismo de Denia....

No julgamento, e depois de um trabalho louvável da Guardia Civil, existe um incompreensível vazio probatório que os próprios membros do Tribunal denunciam e que tem a seguinte redação: "...Não obstante o exposto, e apesar dos esforços realizados pelo Ministério Público, entendemos que existe um importante vazio probatório que nos obriga a declarar a absolvição do arguido. Um vazio probatório que decorre da falta e ausência de prova de um dado transcendental, como é o caso da autoria da carta manuscrita que o Ministério Público atribui a Melisa, e para a qual não foi produzida qualquer prova. Este vazio probatório deve-se à omissão dos agentes policiais que emitiram o relatório de peritagem de caligrafia, que consta do processo no chamado "Anexo Documental", e onde se analisam detalhadamente os documentos encontrados em França, incluindo a "kantada" atribuída à arguida. Este relatório de peritagem de caligrafia, datado de 20 de maio de 2008 e elaborado por agentes de polícia com as cédulas profissionais n.ºs NUM005 e NUM006, foi ratificado na fase de inquérito perante o Tribunal Central de Instrução, mas posteriormente o Ministério Público não os propôs como prova pericial e, portanto, como não tinham sido "levados" a julgamento, e não tendo sido objeto de contraditório entre as partes, não pode ser considerado como prova contra a arguida, tendo sido expressamente impugnado pela sua defesa, arguida essa que, por outro lado, na sessão plenária, afirmou clara e frontalmente que não reconhecia o documento em causa como seu e que não o tinha redigido. Por outro lado, o relatório 7/2015, um relatório que poderia ser chamado de "relatório de inteligência", que analisa a existência e os componentes do comando da

⁵ SAN 8/2025, Sección Penal 3ª de 02 de abril de 2025, publicada na página web da CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: SAN 1662/2025 - ECLI:ES:AN:2025:1662). Recurso: 132/2010. Interveniente: Jesús Eduardo Gutiérrez Gómez.

ETA conhecido como Ibarla, a sua atividade e os dados sobre os ataques cometidos por este comando terrorista, e a sua comparação com os documentos encontrados em França, Este relatório, que poderia ter esclarecido a eventual autoria da colocação do explosivo no Aeroporto de Alicante, em oposição à negação dos factos pelo arguido, também não foi objeto de prova em plenário, uma vez que os autores do relatório não foram propostos como peritos. Assim, os depoimentos das testemunhas que compareceram no julgamento não têm valor probatório como prova da acusação e como prova da autoria do arguido, uma vez que foi erradamente "presumido" e assumido que a "kantada" era a única prova sólida para a acusação (o depoimento do arguido), (o depoimento policial não tem valor de prova para a acusação, por não ter sido verificado ou ratificado pelo arguido no Tribunal Central de Instrução Prévia) tinha sido redigida pelo arguido, pelo que de pouco nos serve provar as eventuais discrepâncias entre este documento e o depoimento policial, por faltar o requisito ou pressuposto, de que a autoria deste documento tenha sido acreditada.

Por conseguinte, e sem apreciar as outras provas, o arguido deve ser absolvido com todos os requisitos necessários para a absolvição...".

Conclusões.

Trata-se de um depoimento chocante neste RAS nº 8/2025 Secção 3, quando o trabalho policial é impecável e o trabalho na fase de instrução foi mais do que completo. O Ministério Público cometeu um grave erro ao não propor em plenário o depoimento dos agentes que analisaram a documentação do réu e dos autores do laudo pericial de inteligência. Não havia outra opção senão a absolvição.

6 - STS 308/2025, de 2 de abril de 2025. Investigação policial em Espanha decorrente do conhecimento de um IEP emitido pelas autoridades judiciais de outro país por outra infração penal. Presença dos detidos numa busca domiciliária . 6

Antecedentes factuais.

O Tribunal de Instrução n.º 1 de Coín abriu o processo abreviado 22/2022 por delitos contra a saúde pública e posse ilegal de armas contra, entre outros, Clemente, David e Eliseo, que, uma vez concluído, foi remetido para julgamento ao Tribunal Provincial de Málaga, 3.ª Secção. Tendo iniciado o processo abreviado 54/2022, em 23 de novembro de 2022, proferiu a Sentença n.º 362/22, que contém, entre outros, os seguintes factos provados: "...Está provado e assim declarado que as autoridades policiais de Málaga tinham conhecimento de que Clemente, maior de idade, sem antecedentes criminais computáveis, de nacionalidade britânica e sujeito a um mandado de captura internacional emitido pelas autoridades do Reino Unido, poderia estar a residir nesta província, especificamente algures no Vale de Guadalhorce ou Coín. Após as devidas investigações, os agentes de investigação chegaram à conclusão de que poderia estar a residir no endereço xxx da localidade de Coín. Por este motivo, nos dias 3, 4 e 5 de maio de 2022, foi efectuada uma vigilância policial na referida propriedade no endereço xxx em Coín, onde os agentes policiais acabaram por saber com certeza que Clemente estava a viver com outros homens. Concretamente, nos dias indicados, encontravam-se no interior do

⁶ STS 308/2025, Secção Penal 1ª de 02 de abril de 2025, publicado no site da CGPJ, Centro de Documentação Judicial, CENDOJ, (ROJ: STS 1482/2025 - ECLI:ES:TS:2025:1482), recurso: 11312/2023. Interveniente: Sr. Pablo Llarena Conde.

imóvel o referido Clemente, maior de idade e sem antecedentes criminais, juntamente com David e Eliseo, todos eles maiores de idade e sem antecedentes criminais, e Fidel, maior de idade e sem antecedentes criminais computáveis, que entraram no referido imóvel em algum momento entre a noite de 3 de maio, quando foi libertado da prisão, e as 20.35 horas de 5 de maio, quando foi visto a sair do imóvel para ir a um centro desportivo. De todos eles, foram David e Eliseo que saíram do imóvel para fazer as compras necessárias, e fizeram-no utilizando um veículo Volkswagen polo com matrícula inglesa, adoptando medidas de segurança para verificar se estavam a ser seguidos, tais como contornar rotundas ou não estacionar o veículo à porta do imóvel mas nas imediações da casa.

No dia 5 de maio, por volta das 20:35 horas, Clemente, Fidel, David e Eliseo saíram juntos de casa, tendo Fidel trancado a porta da casa, que nessa altura transportava uma mochila preta às costas, que entregou a Clemente pelo caminho. As quatro pessoas acima mencionadas dirigiram-se ao ginásio BlueLife Sportclub and Spa, situado no centro comercial La Trocha, em Coín, altura em que os agentes da polícia intervieram para prender os quatro homens acima mencionados. No momento da detenção, a mochila preta que Fidel trazia às costas à saída da casa foi colocada aos pés de Fidel e Clemente. No interior da mochila, ao ser inspeccionada, foi encontrada uma pistola Ruger P89, calibre 9mm Parabellum, modelo P89, com munições e sem travão de segurança, com o número de série retirado. Após a análise pertinente, verificou-se que se encontrava em bom estado de conservação e que o seu funcionamento mecânico e operacional estava igualmente correto, tanto em ação simples como dupla, estando apta a disparar. Nem o Fidel, nem o Clemente, nem o David, nem o Eliseo possuíam licença para esta arma.

Em 6 de maio de 2022, o tribunal de Coín emitiu uma ordem que autorizava a entrada e a busca na casa do endereço xxx em Coín por ordem de 6 de maio de 2022, na qual foi encontrada uma grande quantidade de estupefacientes...".

Base jurídica

É surpreendente que a defesa dos arguidos não tenha suscitado a eventual nulidade dos actos praticados pela Polícia Judiciária, quando, sabendo da existência de um mandado de detenção europeu, iniciou uma investigação e não procedeu à detenção imediata da pessoa procurada. Nada é dito no acórdão, e melhor, porque avaliza todo o trabalho policial, que é imediatamente comunicado ao juiz de instrução, que até concorda com a entrada e busca domiciliária para o ato praticado em Espanha. Como veremos, a decisão do Tribunal Provincial de Málaga foi condenatória e o Supremo Tribunal negou provimento ao recurso de cassação.

Esta é a informação do processo que é transferida para o Tribunal de Coín e que tantas vezes vemos na prática, por exemplo, a existência não só do OEDE mas de buscas e apreensões a nível nacional, o que nos levaria a pensar na necessidade imediata de prender, quando nem sempre é esse o caso, como vemos neste STS.

Os recorrentes alegam que o procedimento de busca e entrada realizado em 6 de maio de 2022 na casa localizada no endereço xxx na cidade de Coín é nulo e sem efeito, porque sendo a residência habitual dos quatro acusados e estando todos eles sob custódia, os agentes da polícia apenas levaram Fidel para estar presente no procedimento de busca e entrada. Por conseguinte, consideram que os resultados desta investigação são nulos e

que não podem ser utilizados como prova legítima da acusação, e que devem ser absolvidos por não existirem outras provas que estabeleçam a responsabilidade dos recorrentes.

Nos acórdãos proferidos por esta Câmara 420/2014, de 2 de junho, ou 508/2015, de 27 de julho (caso Malaya), citando outros precedentes, resumimos a nossa doutrina sobre a exigência da presença do interessado na prática da entrada e da busca no domicílio.

Neles dizíamos que o fundamento da exigência da presença do interessado ou do seu representante na entrada e busca domiciliária ordenada pela autoridade judiciária em processo penal reside, por um lado, no facto de este procedimento afetar um direito pessoal, de natureza constitucional, que é o direito à intimidade pessoal, uma vez que o domicílio constitucionalmente protegido, enquanto habitação ou moradia de uma pessoa, está intimamente ligado à sua esfera de intimidade, pois o que se protege não é apenas um espaço físico, mas também a emanção de uma pessoa física e a sua esfera privada (STC 188/2013, de 4 de novembro, em relação a art. 18 2.º CE e art. 8.º da CEDH). Em segundo lugar, afecta o direito a um julgamento justo, porque o resultado deste procedimento constituirá prova no julgamento contra o arguido cuja casa foi revistada, o que significa que a busca deve ser conduzida de forma a garantir a validade da busca como prova pré-constituída.

A lei processual prevê, assim, como requisito para a prática da busca, a presença do interessado ou de quem legalmente o represente (art. 569.º da LECrim). E o interessado a que se refere o artigo 569.º da LECrim não é necessariamente o proprietário, no sentido de possuidor ou arrendatário do imóvel. O que é decisivo não é quem é o proprietário, que pode ser desconhecido, não residir na casa, ou mesmo ser uma pessoa colectiva, mas quem é o residente na casa, pois é a sua privacidade que vai ser afetada.

Normalmente, a pessoa interessada na busca é o arguido, uma vez que o resultado da busca afectará a sua defesa, embora nem sempre tenha de ser necessariamente o arguido a estar presente na busca legalmente autorizada. O arguido ou a pessoa contra quem se dirige o processo pode estar desaparecido ou simplesmente fora do domicílio e não ser localizável no momento da busca. A entrada e a busca domiciliária autorizadas no âmbito de um processo judicial por infração penal é, pela sua própria natureza, um procedimento urgente que não pode ser adiado enquanto se aguarda que o arguido regresse a casa ou seja localizado pela polícia. Por isso, a lei autoriza que se dispense o interessado "quando este não estiver presente", o que se refere claramente ao arguido, podendo, nestes casos, a busca ser efectuada na presença de qualquer um dos seus familiares maiores de idade, considerando a doutrina jurisprudencial, tendo em conta uma realidade social em que os agrupamentos de casas já não são necessariamente realizados por famílias em sentido estrito, que esta regra é aplicável a todos os habitantes da casa, maiores de idade, mesmo que não sejam familiares em sentido estrito.

No entanto, o que se exige é a presença do arguido na busca quando este se encontra detido ou sob custódia policial ou judicial, pois nestes casos não se justifica prejudicar o seu direito ao contraditório, que é melhor garantido pela presença efectiva do arguido na busca.

Em todo o caso, recordámos também nestes acórdãos que esta regra não é aplicável aos casos de força maior, em que a ausência do arguido, apesar de estar à disposição da

polícia, é justificada. Citámos como exemplo os casos de hospitalização do arguido, ou de detenção em local afastado do domicílio, ou no caso de buscas efectuadas simultaneamente em vários domicílios. E também quando a impossibilidade da sua presença é de natureza legal, por exemplo quando a investigação foi declarada secreta (STS 143/2013, 28 de fevereiro).

E quando há vários moradores na residência, nas nossas SSTs 336/2017, de 11 de maio ou 913/2023, de 13 de dezembro, recordando as SSTs 698/2002, de 17 de abril, 1108/2005, de 22 de setembro, 352/2006, de 15 de março, 684/2014, de 2 de outubro ou 79/2015, de 13 de fevereiro, sublinhamos que a validade e a eficácia do procedimento de entrada e revista não são afectadas pela presença de um dos residentes, desde que este não tenha interesses conflitantes com os dos outros arguidos. Sem prejuízo de, nestes casos, não obstante a validade da busca e para garantir o respeito pelo direito ao contraditório, que integra o mais amplo direito de defesa, a busca não pode ser considerada como prova pré-constituída, sendo necessário que, para além da mera leitura do auto lavrado durante a sua realização, as testemunhas que se aproximaram ou presenciaram a sua prática compareçam para depor em sede de julgamento oral.

Por conseguinte, os fundamentos são julgados improcedentes.

Sem prejuízo do facto de, no caso em apreço, a condução e a detenção de todas as pessoas privadas de liberdade terem afetado a disponibilidade do pessoal da polícia destacado para a pequena cidade onde os recorrentes exerciam as suas actividades criminosas e onde se encontravam detidos, uma vez que teria sido necessário um elevado número de agentes para a transferência e a vigilância dos quatro arguidos e para a realização da investigação, uma análise objetiva das circunstâncias concomitantes permitiu aos investigadores concluir que não existia qualquer contradição de interesses entre as pessoas objeto da investigação. Concretamente, o sistema de vigilância da polícia, montado durante três dias para vigiar os habitantes da casa durante um longo período de tempo, permitiu estabelecer que todos eles eram residentes na casa e que actuavam em conjunto. Em particular, David e Eliseo, quando saíram da casa de carro, tomaram medidas de segurança para verificar se estavam a ser seguidos. E tanto eles como os outros detidos agiam por vezes de forma concertada, chegando mesmo a trocar objectos como uma mochila. E esta presumível ausência de interesses contraditórios foi confirmada pelas quantidades significativas de substâncias estupefacientes apreendidas e pelo número e localização das armas apreendidas, uma vez que a prova testemunhal, contraditada em sessão plenária, mostra que a droga era visível para todos os habitantes da casa e não estava escondida em nenhuma divisão destinada ao uso exclusivo de qualquer um deles, excluindo assim a possibilidade de um responsável tentar transferir a responsabilidade exclusiva para os outros residentes. Assim, foram também apreendidas as três pistolas, o que levou à sua condenação como autores do crime de posse ilegal de armas.

Conclusões.

Depois de endossar a investigação num caso que se baseou no conhecimento policial de um IEP emitido pelas autoridades judiciais do Reino Unido por um ato criminoso diferente, e sem que a Defesa tenha contestado a possível omissão do dever de processar crimes pelo FCSE ao não prender imediatamente a pessoa abrangida pelo IEP em vigor, e evitando assim a investigação iniciada no Tribunal de Coín, este STS 308/2025 fornece

uma descrição fenomenal e didática de quem goza do conceito de parte interessada numa entrada e busca numa casa, quer a pessoa seja ou não detida, estabelecendo uma regra geral e as excepções em casos extraordinários. Também delimita o possível conflito de interesses entre os afectados.

7- STS 295/2025, Secção Penal 1ª de 28 de março de 2025, crime de assédio, "stalking".⁷

Antecedentes factuais.

O Tribunal de Violência contra a Mulher nº 1 de Medio Cudeyo, abriu o processo urgente nº 36/2021, uma vez concluído foi enviado ao Tribunal Penal nº 5 de Santander, para julgamento no processo de julgamento rápido nº 125/2021, que emitiu a Sentença nº 285/2021, datada de 25 de novembro de 2021, que contém os seguintes fatos comprovados: "...Ficou provado que o arguido Basílio, maior de idade, e sem antecedentes criminais computáveis para efeitos de reincidência, que manteve uma relação sentimental durante um ano com Concepción, com morada em Iruz (Santiurde de Toranzo), que cessou em julho de 2020, desde outubro desse ano telefonou-lhe, enviou mensagens de WhatsApp e cartas insistentemente, pedindo-lhe perdão e pedindo-lhe que retomasse a relação, dizendo "a minha vida não tem sentido, que estava a pensar na melhor maneira de desaparecer, o que vou fazer agora, que a vida não tem sentido para mim", tendo sido encontrado às 09:00 horas do dia 15 de dezembro. Às 00 horas do dia 15 de dezembro foi encontrado sentado numa cadeira no seu jardim semi-consciente com os olhos revirados na cabeça e teve de ser evacuado para o hospital, vindo no dia 1 de janeiro de 2021 a sua casa bater à porta, passando a telefonar-lhe constantemente e a enviar-lhe uma carta por mês, tudo com a intenção de alterar gravemente a sua vida, apesar de ter conhecimento de que Concepción não quer manter qualquer tipo de relação com ele...".

A 3ª Secção do Tribunal Provincial de Santander deu provimento ao recurso do condenado e absolveu-o, tendo o representante da vítima interposto recurso de cassação, ao qual foi dado provimento, condenando novamente o arguido.

Base jurídica.

Dada a natureza marcante das pronúncias judiciais, condenação em primeira instância, absolvição em recurso e condenação novamente em recurso, a jurisprudência do TEDH admite a revisão das absolvições quando o Supremo Tribunal actua dentro das margens da violação da lei, revendo questões meramente jurídicas. Ou seja, quando esta Secção se limita a corrigir erros de subsunção e a estabelecer critérios interpretativos uniformes para garantir a segurança jurídica, a previsibilidade das decisões judiciais, a igualdade dos cidadãos perante a lei penal e a unidade do sistema penal e processual penal, sem alterar quaisquer pressupostos de facto.

O artigo 172.º, n.º 3, do Código Penal, em vigor à data da prática dos factos - uma vez que o preceito foi reformado pela LO 1/2023, de 28 de fevereiro -, pune

⁷ STS 295/2025, Secção Penal 1ª de 28 de março de 2025, delito de acoso, "stalking", publicado no site da CGPJ, Centro de Documentação Judicial, CENDOJ, (ROJ: STS 1348/2025 - ECLI:ES:TS:2025:1348), recurso: 7251/2022. Intervém a Exma. Sra. Susana Polo García.

expressamente quem "assediar uma pessoa, praticando, de forma insistente e reiterada, sem estar legitimamente autorizado a fazê-lo, qualquer das seguintes condutas e, desse modo, alterar gravemente o desenvolvimento da sua vida quotidiana". O referido artigo, que define o crime de assédio, foi introduzido no Código Penal pelo Decreto-Lei n.º 1/2015, de 30 de março de 2015. 1/2015, de 30 de março, cuja Exposição de Motivos refere que "trata de "todos os casos em que, sem envolver necessariamente o anúncio explícito ou não explícito da intenção de causar dano (ameaças) ou o uso direto de violência para restringir a liberdade da vítima (coação), se verifiquem condutas reiteradas através das quais a liberdade e o sentimento de segurança da vítima sejam gravemente postos em causa, ficando esta sujeita a perseguição ou vigilância constantes, telefonemas repetidos ou outros actos contínuos de assédio".

Nestes termos, a Jurisprudência tem-se pronunciado desde o Acórdão do Plenário 324/2017, de 8 de maio, e 554/2017, de 12 de julho, este último com remissão expressa para o anterior, onde se afirma, entre outras coisas, que, portanto, pode afirmar-se que de forma insistente e reiterativa equivale a dizer que estamos perante uma reiteração de acções da mesma natureza - um continuum - que se repete no tempo, num período não especificado no tipo, pode afirmar-se que de forma insistente e reiterativa equivale a dizer que estamos perante uma reiteração de acções da mesma natureza - um continuum - que se repete no tempo, num período não especificado no tipo penal, e que estamos na presença de um tipo penal muito "agarrado" aos perfis e circunstâncias específicas do caso em julgamento. Por outras palavras, a análise de cada caso concreto, tendo em conta as acções realizadas pelo agente com insistência e reiteração e, por outro lado, tendo em conta a idoneidade de tais acções para alterar gravemente a vida e a paz de espírito da vítima, levar-nos-á à existência ou não de tal crime de assédio, cabendo a este Tribunal de Cassação, uma vez que o recurso se baseia na dupla instância - sentença do Tribunal Penal e sentença de recurso ditada pelo Tribunal Provincial - determinar se, perante os factos provados, existem ou não os elementos que constituem a espinha dorsal do crime.

Por outro lado, para além da definição legal, existem definições do fenómeno na comunidade científica, fundamentalmente no domínio da psicologia e da psiquiatria, que, regra geral, o definem como comportamentos que um indivíduo inflige a outro através de intrusões ou comunicações não desejadas, identificando a intrusão com o facto de perseguir, rondar, pairar, vigiar, aproximar-se, e comunicar com comportamentos como enviar cartas, fazer telefonemas, enviar e-mails, grafitar ou anotar no carro, ou comportamentos associados como encomendar serviços em nome da vítima, fazer falsas acusações, etc., exigindo sempre que estes comportamentos sejam repetitivos ou reiterativos.

O artigo 172.º-ter descreve o ilícito penal, em termos gerais, utilizando o verbo "assediar", termo sobre o qual não existe consenso no nosso ordenamento jurídico quanto à sua definição, nomeadamente quanto à necessidade de tantos actos quantos os necessários, mas não podemos ignorar que o assédio sexual e o assédio em razão do sexo não carecem de repetição ou persistência, de acordo com o conceito do mesmo no artigo . 7.1 e 7.2 da Lei Orgânica n.º 3/2007, de 22 de março, para a igualdade efectiva entre mulheres e homens, e a introdução na nossa lei penal do crime de stalking, é mais uma resposta ao combate à violência de género e ao cumprimento das normas internacionais e mais concretamente da Convenção de Istambul.

Importa ainda ter presente que o legislador, e bem, a nosso ver, não determina o número de ocasiões em que a conduta assediante deve ocorrer, nem o período de tempo em que deve ocorrer, e quanto à alteração grave da vida quotidiana, dissemos que o crime não exige planeamento, mas sim uma sequência metódica de acções que obriguem a vítima, como única saída, a alterar os seus hábitos quotidianos. Para avaliar a idoneidade da ação sequenciada para alterar os hábitos quotidianos da vítima, deve ter-se em conta o padrão do "homem médio", embora este seja qualificado pelas circunstâncias específicas da vítima (vulnerabilidade, fragilidade psicológica, etc.) que não podem ser totalmente ignoradas (STS 639/2022, de 23 de junho).

Prevemos que o recurso seja julgado procedente, com a consequente anulação da absolvição e a sua substituição por uma condenação.

O relato dos factos provados descreve a conduta do arguido, que, durante um período de pelo menos três meses, telefonou repetidamente à sua ex-companheira, enviou-lhe mensagens de WhatsApp e cartas, insistentemente, segundo o relato, em todas elas pedindo perdão e solicitando à sua ex-companheira que retomasse a relação que tinha cessado meses antes, dizendo "a minha vida não tem sentido, que estava a pensar na melhor maneira de desaparecer, o que vou fazer agora, que a vida não tem sentido para mim", um dia, a vítima chegou a encontrá-lo sentado numa cadeira no seu jardim "semiconsciente, com os olhos virados para trás e teve de ser evacuado para o hospital", deslocando-se a casa de Concepción 15 dias depois, batendo à porta, e voltando a telefonar-lhe constantemente e a enviar-lhe uma carta por mês, com a referida intenção de reatar a relação, apesar de saber que Concepción não queria manter qualquer tipo de relação com ele.

O crime de perseguição protege a liberdade individual e o direito de viver em paz e sem preocupações. As mensagens, a comparência em casa da vítima mostrando a sua tentativa de suicídio para a responsabilizar, bem como os telefonemas e mensagens enviadas, são, por si só, susceptíveis de perturbar os hábitos, costumes, rotinas ou modo de vida de qualquer pessoa, tendo em conta o padrão do "homem/mulher médio", reflectindo o Tribunal Penal na sua fundamentação que o exposto obrigou a vítima a receber apoio psicológico, facto que não se contesta. Os mesmos actos dos factos provados, -cobrem os requisitos que esta Câmara tem vindo a exigir do tipo do art. 172º ter CP, nomeadamente, insistência, reiteração, repetição, reflexo de um mesmo padrão ou modelo sistemático, existência de uma vontade de perseverar nestas acções intrusivas, ultrapassando em muito o meramente episódico ou circunstancial e falta de legitimação, ou autorização para agir desta forma. Devido ao período de tempo durante o qual são enviadas e ao seu conteúdo, o desvalor que contêm é de um nível muito elevado, suficiente para desencadear uma reação criminosa.

Neste caso, não se trata de um simples comportamento incómodo, as acções descritas no relato dos factos são susceptíveis de alterar a vida e a paz de espírito da vítima de qualquer forma, afectando ou alterando o futuro da vítima de qualquer forma na sua vida privada, no seu trabalho ou nas suas relações com terceiros. Em suma, Concepción foi objeto de chantagem emocional, entendida como uma forma de comunicação que visa manipular uma pessoa em detrimento de outra, recorrendo ao medo, à obrigação e, sobretudo, neste caso, à culpa.

Estamos perante factos que implicam uma clara submissão psicológica, em que o arguido subjuga psicologicamente a sua ex-companheira com a ideia de que não vai parar enquanto não voltar para ela, responsabilizando-a mesmo pela sua própria vida com a tentativa de auto-mutilação no jardim da casa da vítima, que provoca medo na vítima, alterando gravemente a sua vida quotidiana, sujeita a tratamento psicológico, sem que seja necessária a realização de prova pericial psicológica em julgamento para provar que o psiquismo da vítima foi afetado por esta situação de assédio ou perseguição, e que tal determina uma alteração na sua vida, quando, como no caso em apreço, resulta do próprio relato factual, pois os acontecimentos geraram necessariamente um impacto emocional na vítima - receio pela sua segurança e pela do seu meio - e um impacto no normal desenvolvimento da sua vida quotidiana, com necessidade de tratamento psicológico.

Como dissemos no STS 843/2021, de 4 de novembro, a essência do tipo penal, e sobretudo, relacionada com atos de violência de género, como o assédio na situação de ex-companheiro, deve ser contemplada com uma perspectiva de género, pois uma situação de assédio entre estranhos ou conhecidos não é a mesma que na relação de um parceiro ou ex-companheiro, em que os laços interpessoais criados intensificam as exigências de domínio ou humilhação do assediador sobre a vítima que é ou foi seu parceiro, com o objetivo de criar laços físicos e psicológicos que demonstrem a submissão que o assediador quer transferir para a sua vítima, para que esta não resista ao assédio e volte para ele.

Consequentemente, os factos descritos são adequados para forçar a vítima a mudar o seu modo de vida, com força suficiente para constituir um crime de assédio, tal como definido no artigo 172 ter do Código Penal, pelo que deve ser dado provimento ao recurso e o arguido deve ser condenado como autor do referido crime, às mesmas penas impostas pelo Tribunal Penal, e a sentença acima mencionada deve ser reintegrada.

Conclusões.

Importante precisão terminológica e factual deste tipo de crime, que como bem refere o STS 295/2025, não quantifica o número de actos de assédio necessários para integrar a infração penal, mas que ambientalmente e avaliando todos os indícios como um todo, e não isoladamente, permite a sua apreciação porque o modo de vida da vítima foi alterado, e mais ainda nos casos de violência contra as mulheres.

8 - STS 284/2025, de 27 de março. Abuso sexual de uma jovem de 17 anos com inteligência limítrofe. Danos morais.⁸

Antecedentes factuais.

O Tribunal Penal n.º 6 de Las Palmas de Gran Canaria no processo proveniente do PA com o número 247/2020, instruído pelo Tribunal de Instrução n.º 1 de Telde, por crime de abuso sexual contra Maximino proferiu sentença que contém os seguintes Factos Provados: "...ÚNICO. Fica provado e declarado que o arguido, Maximino, nascido em xx1984, no dia 1 de maio de 2017, à tarde, sem poder precisar a hora, guiado pelo desejo

⁸ STS 284/2025, Seção Penal 1ª, de 27 de março, publicada no sítio Web da CGPJ, Centro de Documentação Judicial, CENDOJ. (ROJ: STS 1469/2025 - ECLI:ES:TS:2025:1469), recurso: 7022/2022. Interveniente: Sr. Antonio del Moral García.

de satisfazer os seus instintos sexuais, convenceu a menor Socorro, de 17 anos de idade, a acompanhá-lo ao prédio sito na morada xxx, e, uma vez lá, tocou-lhe nas nádegas e na coxa, aproveitando-se do facto de ela ser menor e de o seu nível de funcionamento intelectual estar no limite da inteligência normal, tornando-a altamente vulnerável a tornar-se vítima. O representante legítimo da menor alega...".

No recurso, o Tribunal Provincial deu provimento parcial ao recurso por atraso indevido e o Supremo Tribunal confirmou a condenação do Tribunal Provincial.

Base jurídica.

Por um lado, o recorrente alega que os factos são atípicos com base no consentimento da vítima. A descrição do ato não permite concluir pela existência de uma perturbação mental. O acórdão fala de um nível de funcionamento intelectual no limite da inteligência normal. Estando no limite e não abaixo do limite - é sublinhado tipograficamente - não seria possível falar de abuso de perturbação.

O raciocínio não é claro. Por um lado, parece estar-se a argumentar que o arguido não tinha conhecimento desta circunstância. Isto contradiz o facto provado de que tirou partido desta característica, o que implica conhecimento. Isto torna a alegação inviável.

Poderia também significar que, estando no limite da normalidade, se poderia falar de normalidade, o que privaria de apoio a ausência de consentimento.

Este segundo argumento possível joga com a linguagem, ignorando o facto de as locuções "inteligência limítrofe" ou "funcionamento intelectual limítrofe" serem conceitos bem elaborados que exprimem algo mais do que aquilo que se poderia deduzir do seu significado literal estrito. As pessoas com estas características não têm o que se considera ser um nível intelectual médio. São - e isto faz parte do património cultural comum: não se trata de uma questão psiquiátrica, muito menos de tecnicismos jurídicos - pessoas capazes de desenvolver processos de vida, de funcionar e de compreender o mundo, mas que necessitam de apoio adequado, uma vez que o seu baixo QI assim o exige. Têm dificuldades na tomada de decisões e na resolução de conflitos; as suas competências sociais estão diminuídas. A Organização Mundial de Saúde estabelece que a inteligência média se situa entre 85 e 115. As pessoas com inteligência limítrofe são aquelas que se situam um pouco abaixo destes valores: entre 70 e 85. Também não se pode falar de normalidade intelectual. Do ponto de vista penal, estão abrangidas pelo conceito normativo de art. 25.1 CP.

Além disso, os factos provados, como se torna ainda mais claro em algumas partes da argumentação factual, não mencionam qualquer consentimento da menor para os toques com implicações sexuais. Não se diz que ela os tenha consentido. Foram-lhe impostos até conseguir fugir, mas sem recurso a violência ou intimidação. De facto, o acórdão não cita o n.º 2 do artigo 181.º (abuso de perturbação mental).

A prática de actos sexuais sem o consentimento da outra pessoa é, por si só, típica, independentemente do nível intelectual da vítima. Se, além disso, a vítima apresentar défices intelectuais que a tornem particularmente vulnerável, o facto será agravado.

A segunda linha de recurso procura afastar esta agravação, considerando-a inerente ao abuso de uma perturbação mental ou alheia ao conhecimento do arguido.

Só através da deturpação dos factos provados se pode argumentar que o arguido desconhecia a especial vulnerabilidade decorrente da inteligência limítrofe que explorava. De resto, a sequência dos factos e a forma como são recriados na fundamentação jurídica são extremamente expressivas.

Se se tratasse de um caso em que se obtém o consentimento, expresso ou exteriorizado por actos concludentes, da vítima, e a tipicidade assentasse em lidar com um consentimento não livre por ausência de capacidade para o dar e com o agente a aproveitar-se do défice cognitivo para o obter, o problema da compatibilidade do art. 181.º, n.º 2 supra (abuso de perturbação mental) ou do art. 178.2 em vigor (abuso de uma situação de vulnerabilidade da vítima) com a agravação específica (especialmente vulnerável devido a... idade, doença, deficiência ou situação: art. 180.1.3º e 181.5 na legislação aplicada; ou especial vulnerabilidade devido a... deficiência ou qualquer outra circunstância: art. 180.1.3º após a LO 10/2022). Mas não é este o caso.

Por um lado, há uma ausência de consentimento. Não estamos perante um consentimento que não é livre por ter sido obtido de forma abusiva. Por outro lado, parece que a vítima tem uma capacidade intelectual diminuída que a torna particularmente vulnerável.

A criminalização foi, portanto, correta.

E o que sobressai do STS é o conceito e o alcance dos danos não pecuniários, tão difíceis de ver na prática quotidiana dos nossos tribunais.

Tanto é assim que o art. 193 CP contém uma prescrição, nas condenações por crimes contra a liberdade sexual, para além da pronúncia correspondente à responsabilidade civil, haverá, quando for caso disso, as correspondentes à filiação e alimentos, o que vem representar uma presunção legal (assente numa máxima de experiência partilhada e indubitável) de dano moral neste tipo de crime (vid SSTs 327/2013, de 4 de março; 1033/2013, de 26 de outubro; 733/2016, de 5 de outubro; 812/2017, de 11 de dezembro; 393/2020, de 15 de julho; 1040/2021, de 26 de outubro ou 1209/2021, de 2 de dezembro).

A recorrente não tem dúvidas de que a indemnização seria igualmente concedida nos tribunais civis se a ação tivesse sido reservada para esse domínio.

Embora não seja aplicável por não estar em vigor à data dos factos, é pertinente referir a regulamentação desta matéria na Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, uma vez que subscreve, com novos aditamentos, a inescusabilidade desta indemnização, decompondo conceitos em que se destacam o dano moral e o dano à dignidade.

Isto é afirmado em art. 53 da lei acima mencionada, sob o título Indemnização.

"1 - A indemnização por danos materiais e morais que corresponda às vítimas de violência sexual, nos termos da legislação penal sobre responsabilidade civil derivada do

crime, deve garantir a satisfação economicamente avaliável de, pelo menos, os seguintes conceitos

(a) danos físicos e psicológicos, incluindo danos morais e danos à dignidade.

(b) Perda de oportunidades, incluindo oportunidades de educação, emprego e benefícios sociais.

(c) danos materiais e perda de rendimentos, incluindo perda de lucros.

d) Dano social, entendido como dano ao projeto de vida.

e) Tratamentos terapêuticos, sociais e de saúde sexual e reprodutiva.

2. A indemnização é paga pela pessoa ou pessoas civil ou criminalmente responsáveis, em conformidade com a regulamentação em vigor".

Conclusões.

O presente STS 284/2025 versa sobre duas questões de interesse. Por um lado, o perfeito enquadramento da figura agravada nos crimes contra a liberdade sexual, quando tenha havido falta de valor na ação do agressor que não é apenas objetiva, actos de toque, mas tem também uma perspetiva subjectiva relevante, aproveitando-se conscientemente da vulnerabilidade da vítima. Por outro lado, o quase esquecido conceito de dano moral, que embora já existisse anteriormente em inúmeros pronunciamentos judiciais, teve seu reconhecimento expresso na polémica LO 10/2022 de garantia integral da liberdade sexual.



Revista Científica
del Centro Universitario
de la Guardia Civil

Revista
Lógos
Guardia Civil

