INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

A investigação do crime de tráfico de estupefacientes através da Internet pela Polícia de Segurança Pública

Rui Miguel da Rocha Rodrigues Lopes da Cruz

Dissertação de Mestrado em Ciências Policiais

Área de especialização em Gestão da Segurança

Orientação científica:

Prof. Doutor Luís Manuel André Elias

Outubro, 2022

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

A investigação do crime de tráfico de estupefacientes através da Internet pela Polícia de Segurança Pública

Rui Miguel da Rocha Rodrigues Lopes da Cruz

Dissertação de Mestrado em Ciências Policiais

Área de especialização em Gestão da Segurança

Dissertação apresentada no Instituto Superior de Ciências Policiais e Segurança Interna, para cumprimento dos requisitos necessários à obtenção do grau de mestre em Ciências Policiais na especialização em Gestão da Segurança, elaborada sob a orientação científica do Professor Doutor Luís Manuel André Elias, Superintendente da Polícia de Segurança Pública/Oficial de ligação junto da Agência da União Europeia para a Cooperação Policial (Europol).

FICHA TÉCNICA

Estabelecimento de Ensino: Instituto Superior de Ciências Policiais e Segurança Interna

Curso: XIII Curso de Mestrado em Ciências Policiais na especialização em Gestão da Segurança

Orientador: Professor Doutor Luís Manuel André Elias

Título: A investigação do crime de tráfico de estupefacientes através da Internet pela Polícia de Segurança Pública

Autor: Rui Miguel da Rocha Rodrigues Lopes da Cruz

Local de Edição: Lisboa

Data de Edição: outubro de 2022

AGRADECIMENTOS

O trabalho que ora se verte resulta de alguns meses de esforço e dedicação e não teria sido possível sem o apoio e motivação de algumas pessoas, às quais o meu reconhecimento torno público.

Ao meu orientador, Professor Doutor Luís Manuel André Elias, pela indicação do caminho a percorrer e pela inexcedível disponibilidade e predisposição fornecida ao longo de todo o trabalho.

Ao Mestre Luís Guerra pela disponibilidade demonstrada e pelo apoio metodológico prestado, sem o qual este trabalho nunca atingiria a qualidade formal desejada.

Ao Instituto Superior de Ciências Policiais e Segurança Interna, minha casa Mãe, por todo o apoio prestado, desde a coordenação ao secretariado deste Curso de Mestrado, cujo reconhecimento público não poderia deixar de frisar.

A todos aqueles que sempre me apoiaram e que vezes sem conta ouviram as ideias que alimentava para elaboração deste trabalho.

À minha família que ao longo da minha formação sentiram a minha ausência.

Para todos, aqui fica a nossa gratidão.

Lisboa, 30 de outubro de 2022

EPÍGRAFE

“Hoje, paradoxalmente, tudo acontece em todo o lugar e, contudo, em lugar nenhum do planeta, mas algures naquilo a que se tem vindo de chamar de ciberespaço…”

(Fernandes, 2013)

ÍNDICE

LISTA DE SIGLAS

ANACOM	Autoridade Nacional de Comunicações
CAAS	Convenção de Aplicação do Acordo Schengen
CNCS	Centro Nacional de Cibersegurança
CG GNR	Comandante-Geral da Guarda Nacional Republicana
COSI	Cooperação Operacional em matéria de Segurança Interna
CPP	Código de Processo Penal
CP	Código Penal
CRP	Constituição da República Portuguesa
DIAP	Departamento de Investigação e Ação Penal
DIC	Departamento de Investigação Criminal
DL	Decreto-Lei
DN PJ	Direção Nacional da Polícia Judiciária
DN PSP	Direção Nacional da Polícia de Segurança Pública
DN SEF	Direção Nacional do Serviço de Estrangeiros e Fronteiras
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EC3	European Cybercrime Centre
EUROPOL	European Law Enforcement Agency
FRONTEX	European Border and Coast Guard Agency
FS	Forças de Segurança
FSS	Forças e Serviço de Segurança
GNI	Gabinete Nacional Interpol
GNR	Guarda Nacional Republicana
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
INTERPOL	International Criminal Police Organization
IOCTA	Internet Organised Crime Threat Assesment
JHA	Justice and Home Affairs
LEA	Law Enforcement Agency
LOIC	Lei de Organização da Investigação Criminal
MO	Modus Operandi
MP	Ministério Público
OAP	Operational Action Plans

OCG	Organised Crime Group
OEDT	Observatório Europeu da Droga e da Toxicodependência
ONU	Organização das Nações Unidas
OPC	Órgão de Polícia Criminal
PGDL	Procuradoria-Geral Distrital de Lisboa
PUC-CPI	Ponto Único de Contato – Cooperação Policial Internacional
PSP	Polícia de Segurança Pública
RASI	Relatório Anual de Segurança Interna
RED	Relatório Europeu sobre Drogas. Tendências e evoluções
SICAD	Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências
SG SSI	Secretário-Geral do Sistema de Segurança Interna
SOCTA	Serious and Organised Crime Threat Assessment
SIS	Sistema de Informação Schengen
TRP	Tribunal da Relação do Porto
TRL	Tribunal da Relação de Lisboa
UCIC	Unidades de Coordenação e Intervenção Conjunta
UNE	Unidade Nacional Europol
UE	União Europeia
V. G.	Por exemplo

RESUMO

A criminalidade organizada cometida através do ciberespaço, em especial o tráfico de substâncias estupefacientes, com utilização de plataformas *online* e diversas ferramentas tecnológicas, é um flagelo reconhecido ao nível nacional e internacional.

Em face do sobredito, considerando o derrube de fronteiras tecnológicas pelos grupos organizados de criminosos transnacionais, exige-se um esforço robusto por parte das Autoridades nacionais e internacionais em ordem a melhor prevenir e combater as novas formas de cibercriminalidade, pois as tendências mostram-nos que atualmente inexiste criminalidade organizada sem utilização de plataformas *online* e ferramentas tecnológicas.

No que concerne ao cibertráfico consideramos pertinente expandir o âmbito de aplicação da Lei do Cibercrime, com utilização *tout court* por parte dos OPC dos meios processuais ali previstos e, por outro lado, rever a LOIC, por forma a que a repartição formal de competências não seja um óbice no combate ao crime de tráfico de estupefacientes *online*.

Do mesmo modo, consideramos mister que a Polícia de Segurança Pública acompanhe a evolução tecnológica, com olhares digitais, de forma a conseguir acompanhar a grande evolução tecnológica, sempre bem aproveitada pelos grupos organizados de criminosos, ao mesmo tempo que se impõe uma atualização de atribuições e competências à Polícia, de forma a acompanhar outras polícias modernas e evoluídas que operam no sistema de segurança interna nacional.

Colhendo os argumentos avançados neste trabalho, concatenados com uma melhor coordenação policial interna e, subsequentemente, internacional, a Polícia ficará em condições de melhor prevenir e investigar o tráfico de substâncias ilícitas com recurso a ferramentas tecnológicas, indo de encontro aos anseios demonstrados nos diversos relatórios nacionais e internacionais emitidos pelas Autoridades competentes na matéria.

Palavras-chave: Criminalidade organizada transnacional; Ciberespaço; Cibercrime; Cibertráfico; Competências de investigação; Internet; Polícia de Segurança Pública

ABSTRACT

Organized crime committed through cyberspace, in particular the trafficking of narcotic substances, using online platforms and various technological tools, is a nationally and internationally recognized scourge.

In view of the above, considering the overthrow of technological borders by organized groups of transnational criminals, a robust effort is required on the part of national and international authorities in order to better prevent and combat new forms of cybercrime, as trends show us that currently there is no organized crime without the use of online platforms and technological tools.

With regard to cyber-trafficking, we consider it pertinent to expand the scope of application of the Cybercrime Law, with tout court use by the Criminal Police Bodies of the procedural means provided therein and, on the other hand, to review the Law on the organization of criminal investigation, in order to that the formal division of competences is not an obstacle in the fight against the crime of trafficking in narcotics online.

Likewise, we consider it essential that the Public Security Police follow technological developments, with digital eyes, in order to be able to keep up with the great technological evolution, always well used by organized groups of criminals, while at the same time imposing an update of attributions. and competences to the Police, in order to accompany other modern and evolved police forces that operate in the national internal security system.

Harvesting the arguments advanced in this work, linked to better internal and, subsequently, international police coordination, the Police will be in a position to better prevent and investigate the trafficking of illicit substances using technological tools, meeting the wishes shown in the various reports. national and international documents issued by the competent authorities in the matter.

Keywords: Transnational organized crime; Cyberspace; Cybercrime; Cyber trafficking; Police investigation skills; Internet; Public Security Police

INTRODUÇÃO

O tema que nos propomos tratar insere-se no âmbito da criminalidade organizada, especificamente no que concerne ao crime de tráfico de estupefacientes cometido através da internet.

Neste sentido, tratando-se de um tipo criminal de prática continuada e reiterada, em que se verifica o seu cometimento conjuntamente com diversas tipologias que se inserem no grupo da criminalidade organizada e grave, pretendemos efetuar um estudo crítico relativo ao tráfico de estupefacientes, inserido no seu todo, mas com especial acento tónico no seu cometimento através de sistemas informáticos e ligações *online*, tendo em consideração a grande evolução tecnológica ocorrida principalmente nas últimas duas décadas, tanto a nível global como em Portugal, evolução essa que tem sido utilizada por grupos organizados de criminosos, que desenvolvem a sua atividade delituosa utilizando diversas ferramentas e sistemas modernos de comunicação *online*, cujo aproveitamento tem sido altamente remuneratório.

O móbil deste trabalho, com especial enfoque para o trabalho que a Polícia de Segurança Pública desenvolve no contexto da investigação criminal em Portugal, compatibiliza-se com a inserção legislativa relativa à repartição de competências de investigação, ocorrida no início deste século, através da Lei n.º 21/2000, de 10 de agosto[1] (Lei [de Organização] da Investigação Criminal), mas cujas raízes não é alheio o Decreto-Lei n.º 81/95, de 22 de abril (Brigadas Anticrime e Unidades Mistas de Coordenação), que veio empenhar no esforço direto de combate ao tráfico de estupefacientes outros órgãos de polícia criminal, criando para o efeito as brigadas anticrime e de unidades mistas de coordenação, integrando a Polícia Judiciária, a Guarda Nacional Republicana, a Polícia de Segurança Pública, o Serviço de Estrangeiros e Fronteiras e Direção-Geral das Alfândegas, numa altura em que – precisamente – o acordo Schengen havia acabado de entrar em vigor em Portugal (26 de março de 1995), deixando de haver fronteiras internas no país com os restantes países da Europa, integrantes do acordo.

[1] Revogada pela Lei n.º 49/2008, de 27 de agosto – Lei de Organização de Investigação Criminal.

Com estes dois elementos, fim das fronteiras internas com os países do espaço Schengen e com a acelerada evolução tecnológica ocorrida, com franco aproveitamento pelos grupos de criminosos organizados, verifica-se a amálgama impetuosa para a criminalidade altamente organizada prosperar, incumbindo às autoridades competentes adotar estratégias eficazes de combate a esta nova realidade.

Em Portugal o regime jurídico relativo ao tráfico de estupefacientes encontra-se previsto no Decreto-Lei n.º 15/93, de 22 de janeiro[2], entretanto atualizado por diversas vezes (29.ª versão – Lei n.º 25/2021, de 11 de maio).

Conforme referido no seu preâmbulo, este diploma, baseado que estava na Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas de 1988, da qual Portugal faz parte integrante[3], tem essencialmente como objetivos principais privar aqueles que se dedicam ao tráfico de estupefacientes do produto das suas atividades, adotar medidas adequadas ao controlo e fiscalização dos precursores, produtos químicos e solventes, substâncias utilizáveis no fabrico de estupefacientes e de psicotrópicos, colmatar "brechas" e potenciar os meios jurídicos de cooperação internacional em matéria penal, bem como organizar, no plano interno, as tabelas de substâncias consideradas ilícitas, remetidas sistemicamente para os anexos deste diploma.

Pese as diversas alterações legislativas que o diploma originário tem vindo a sofrer, o regime, previsto e punido pelo artigo 21.º e seguintes, não prevê *in concreto* o tráfico de estupefacientes através da internet, através da utilização de plataformas *online*, ressaltando à vista a necessidade de, em face da evolução tecnológica que temos vindo a assistir, reiteradamente aproveitada pelos grupos organizados de criminosos, atualizar o referido diploma.

Torna-se, igualmente, cada vez mais importante que as Autoridades competentes disponham de mecanismos para detetar e investigar atividades de tráfico de estupefacientes por via *online*, exigindo-se um esforço permanente

[2] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=181&tabela=leis.
[3] Convenção assinada e ratificada internamente através da Resolução da Assembleia da República n.º 29/91 e Decreto do Presidente da República n.º 45/91, publicados no Diário da República, de 6 de setembro de 1991.

para acompanhar a atividade criminosa de tráfico de estupefacientes com utilização tanto de canais e plataformas inseridas na internet "aberta" (*surface web*) como de canais inseridos na internet profunda (*Deep web*), de modo a prevenir, reprimir e combater este tipo de criminalidade.

Para fazer face à criminalidade informática em geral e combater o cibercrime, em 2009 foi aprovada a Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro[4], relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre o Cibercrime do Conselho da Europa.

Destaca-se nesta Lei as disposições materiais e processuais, aplicáveis a crimes cometidos por meio de sistema informático, bem como as disposições atinentes à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, relevando para este trabalho a discussão de saber se se pode considerar o crime de tráfico de estupefacientes cometido através da internet como um crime cometido "por meio de um sistema informático", relevando a distinção entre criminalidade informática e criminalidade com recurso a meios informáticos (Verdelho et. al. (2013).

Em outro patamar, parece-nos justo afirmar que a Polícia de Segurança Publica, num esforço contínuo de adaptação às novas realidades, em especial tecnológicas, e evolução societária paralela e concomitante, cresceu de forma sustentada a acompanhar a atividade criminosa em Portugal, com grande aposta visível na formação de efetivo especializado ao serviço da investigação criminal.

Deste modo, esta investigação ergue-se como pertinente no sentido em que, após trazermos à colação o estado da arte relativo ao arquétipo em vigor em Portugal no que toca à investigação da criminalidade organizada num mundo global e evoluído, em especial quanto ao tráfico de estupefacientes cometido através da internet, temos como objetivo discutir criticamente o modelo em vigor no sentido de almejarmos identificar anacronismos e óbices

[4] Lei n.º 109/2009, de 15 de setembro, que aprovou a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de segurança de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa).

ao seus sucesso, em ordem a apresentar propostas que concorram para a sua melhoria, eficiência e eficácia.

Tendo em consideração a sobre referida Lei do Cibercrime, que prevê mecanismos que potenciam a recolha de prova, no domínio do cibercrime, em suporte eletrónico, cumpre-nos averiguar da aplicabilidade deste regime ao tráfico de estupefacientes cometido através da internet e, como questão derivada, saber como articular a aplicabilidade do regime considerando o quadro atual de repartição de competências, entre os Órgãos de Polícia Criminal, previsto em Portugal.

De facto, a sociedade tornou-se invisível, hoje tudo tem uma dimensão digital, sendo que os criminosos, não só os que detêm uma estrutura organizada e devidamente hierarquizada, mas também os "criminosos de bairro", aproveitam-se grandemente das redes sociais e digitais para perpetrar o crime (v.g. burlas *mbway*).

Neste sentido, perante sistemas tradicionais de segurança pública – virados para o vulgo "patrulhamento apeado de zona", urge igualmente, perante as novas realidades digitais, discutir novas formas de policiamento, apostando-se na vigilância e policiamento (prevenção) em rede, bem como na recolha da prova digital (investigação criminal), em ordem a mais rapidamente detetar e investigar o crime que cada vez mais ocorre em plataformas digitais, atualmente carente de vigilância policial.

Considerando o objetivo do presente estudo e que "a partir do instante em que se inicia uma investigação (…) é necessário método" (Campenhoudt & Quivy, 2019, p. 28), decidimos desenvolver no processo de pesquisa o método dialético que, conforme nos ensina Lakatos e Marconi (2003), é um método de interpretação abrangente e dinâmico, no sentido em que os factos em estudo não podem ser destacados de todo um contexto social, político e jurídico em que se inserem, pois as "coisas não são analisadas na qualidade de objetos fixos, mas em movimento (…) encontrando-se em vias de se transformar, desenvolver" (Lakatos & Marconi, 2003, p. 101).

Dito de outro modo, pretendemos invocar, na nossa investigação, conhecimentos provenientes das ciências jurídicas e das ciências sociais,

articulados com doutrina policial e jurisprudência existente, de forma a interpretar e analisar o conhecimento bibliográfico e legislativo recolhido, para o transformar num novo produto de conhecimento, após integramos e cruzarmos dados existentes em Relatórios oficiais, nacionais e internacionais, no sentido de conseguirmos alcançar novos entendimentos.

Optamos, pois, por efetuar um estudo teórico, comparticipado por um raciocínio lógico e dedutivo, perante a evolução tecnológica, que atualmente vivenciamos, e estado da arte do atual policiamento digital em rede, através de um método científico de estudo heterogéneo e de natureza compósita, com cruzamento de teorias pré-existentes, conforme referimos anteriormente, que possam permitir que nos atrevamos a colocar em crise o quadro doutrinário e legal atualmente em vigor, à luz de novas conceptualizações que pretendemos adquirir.

Nesse sentido, em face da pergunta de partida referida, tendo em consideração a escassez bibliográfica acerca do tema, que ao contrário do expectável nos motiva de modo desafiante, propomo-nos efetuar uma análise crítica da literatura e da legislação em vigor, revisitar relatórios oficiais, nacionais e internacionais, acerca desta temática, com o objetivo de "dar forma conveniente e representar de outro modo essa informação, por intermédio de procedimentos de transformação" (Bardin, 2020, p. 47), de modo a ficarmos habilitados a responder à nossa questão previamente formulada e, a final, estarmos aptos a efetuar algumas sugestões que possam contribuir para uma mais eficaz e eficiente perspetiva desta temática.

Posto o mencionado, em face do que pretendemos alcançar com o presente estudo, a nossa dissertação terá a seguinte estrutura: introdução, capítulo I sobre a criminalidade organizada e globalização, capítulo II, em que debateremos acerca da coordenação nacional e cooperação internacional em matéria de investigação criminal, capítulo III abordará a prevenção e investigação do crime de tráfico de estupefacientes, capítulo IV sobre o tráfico de estupefacientes cometido através da internet, capítulo V sobre a necessidade de ajustamento legislativo perante novas realidades e a conclusão. De referir que os capítulos delineados não se apresentaram de

forma estanque, pretendendo-se que a sua segmentação obedeça a uma linha de ideias inter-conexionadas entre si, com destaque para uma análise prospetiva da realidade dos factos, em permanente evolução, numa época em que a evolução tecnológica ocorre à velocidade da luz.

No capítulo I procuraremos chamar à atenção às transmutações que a globalização trouxe às sociedades modernas, que potenciadas pela evolução tecnológica e em conjugação com as fronteiras abertas, no espaço Schengen, vieram dar corpo e consolidar novas tendências criminais. Considerando o mencionado, e sem prejuízo das medidas compensatórias existentes, abordaremos a necessidade de os diversos Estados desenvolverem novos entendimentos que permitam minimizar as novas vulnerabilidades expostas pelas novas realidades.

No capítulo II, debruçar-nos-emos acerca da fundamentalidade da cooperação policial internacional na prevenção e combate ao crime organizado, tornando-se necessário, a montante, uma eficiente e eficaz coordenação policial interna, que permita um rápido e fluído intercâmbio de informações entre os Estados e as agências europeias e internacionais com responsabilidades na matéria. Destacaremos, portanto, o importantíssimo papel da Europol, Interpol e Gabinetes Nacionais Sirene, que fornecem informações e apoio na recolha, análise e tratamento de informação criminal entre os diversos Estados, relativas a organizações criminosas. Destacaremos, igualmente, o Centro de Inovação da UE para a segurança interna, que tem como objetivo fornecer soluções tecnológicas aos EM, em ordem a fomentar sinergias comuns, com o desenvolvimento de ferramentas tecnológicas para melhorar a prevenção e repressão do crime organizado cometido através da internet.

No capítulo III abordaremos as atribuições e competências da PSP, enquanto Polícia integral, em especial o papel fundamental que desempenha a prevenção da criminalidade em geral e no seio da investigação criminal, ainda que sustentada por um regime de partilha de competências de investigação rígidas, decorrentes da LOIC. Neste sentido, iremos trazer a lume novas e legítimas visões acerca do âmbito de competências de investigação criminal

que reinam entre os OPC, que permitam melhor prevenir e combater fenómenos criminais com utilização de meios e ferramentas tecnológicas, em face da importância que configura a luta contra a criminalidade ocorrida no ciberespaço.

O capítulo IV versará especificamente acerca do crime de tráfico de estupefacientes cometido online, pelo que focaremos os vários MO recentes neste domínio. Destacaremos o crime de tráfico de estupefacientes tanto ao nível da darknet como através da internet visível, através de redes sociais e canais de comunicação cada vez mais conhecidos e utilizados por todos nós, aproveitados pelos criminosos no cometimento do crime. Em face da grande dificuldade, que entoaremos, na identificação e investigação do cibertráfico, efetuaremos propostas no sentido de se empreendam esforços e capacitem-se as autoridades policiais competentes, para fazer face a esta realidade cada vez mais patente.

O capítulo V incidirá na análise da legislação em vigor – Lei do Cibercrime e LOIC, com o objetivo de a final, ficarmos aptos para propor um novo paradigma perante novas realidades digitais atuais. Em face das previsões anacrónicas nos textos legislativos que incidem sobre esta temática, que se anteveem, discutiremos a eventual necessidade de alterações legais ou compatibilização legal com a prática de investigação criminal que decorre das competências dos OPC, de modo que se garanta ganhos visíveis no combate ao cibercrime, cada vez mais sofisticado e organizado. Iremos, ainda neste capítulo, discorrer acerca da ação concreta do CNSC que possa garantir uma coordenação efetiva dos OPC, no âmbito do cibercrime e, em específico na prevenção e combate ao tráfico de estupefacientes online.

Na conclusão iremos responder à nossa questão de partida, onde nos disporemos a efetuar algumas reflexões e propostas de melhoria acerca do tema em estudo, alinhadas com a nossa vivência profissional enquanto Oficial da PSP, a desempenhar funções no âmago da investigação criminal há cerca de uma década.

CAPÍTULO 1

CRIMINALIDADE ORGANIZADA E GLOBALIZAÇÃO

1.1 – Globalização. Das novas tendências

A globalização, como processo, carateriza-se por uma crescente interdependência económica, social, política e cultural entre os países, regiões e seus povos, cuja aproximação assenta em diversos fatores, nomeadamente no desenvolvimento de uma variedade de novas tecnologias de informação que revolucionam e tornam cada vez mais premente a comunicação, garantem o estabelecimento de redes globais de produção e incentivam a crescente livre circulação (Giddens, 2000).

Neste campo existe a inserção da internet, atualmente de banda larga, que contribuiu sobremaneira para o processo de desenvolvimento cultural entre os povos, aproximando os mesmos, de tal modo que se torna fácil e comum afirmar que o ser humano vive numa "aldeia global" estando uns dos outros à distância de um clique, surgindo o ciberespaço como "um novo *Global Common*, ou seja, um espaço essencial ao funcionamento da nossa sociedade, que é partilhado por todos, embora não pertença a nenhum Estado em particular" (Moniz, 2018, p. 17).

Por outra via, embora os avanços das novas tecnologias tenham contribuído e continuem a contribuir para o desenvolvimento económico, cultural e social de todos os povos do mundo, também existe uma utilização tecnológica que serve os interesses de organizações criminosas organizadas, trazendo-nos diversas formas de criminalidade complexas, as quais os Estados não estavam preparados para lidar *ab initio*.

Deste modo, podemos afirmar que a sociedade em que vivemos hoje, derivado das várias transmutações, nomeadamente científicas e tecnológicas, complexificou-se como resultado da globalização (Lourenço, 2015) e, como explica João Davin, embora as vantagens advenientes do mercado único europeu, que vieram garantir maior fluidez de pessoas, bens e capitais, verifica-se também um "efeito perverso" ao permitir, igualmente, uma maior

itinerância da criminalidade organizada transnacional em aproveitamento, tanto das fronteiras abertas no espaço Schengen como proveito dos díspares ordenamentos jurídicos dos diferentes países de eleição das organizações criminosas (Davin, 2007).

Conforme refere Nelson Lourenço, ao nos dar nota da definição de criminalidade organizada transnacional da ONU (2003), a qual acolhemos, a mesma é vista como um conjunto heterogéneo de atos, focando-se principalmente nos atores e não tanto nas infrações cometidas pelos mesmos, daí se tornar essencial que a sua prevenção e combate seja efetuada de forma global (Lourenço, 2015).

Considerando o paradigma enunciado, tendo em conta a complexificação da criminalidade organizada a que hodiernamente assistimos, verificamos que as entidades com competência na matéria, nacionais e internacionais, utilizam diversas metodologias de atuação no seu combate.

Repare-se, por exemplo, na inexistência no ordenamento jurídico nacional de uma definição direta de "criminalidade organizada" ou, ainda mais especificamente, de criminalidade organizada transnacional, não obstante, entre as várias definições legais que o Código de Processo Penal (CPP) nos oferece, desde logo nas suas disposições preliminares e legais[5], é a de "criminalidade altamente organizada", considerando as condutas que integram crimes de associação criminosa, tráfico de órgãos humanos, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência e participação económica em negócio ou branqueamento.

Este tipo de criminalidade beneficia, nos termos do CPP, de diversas prerrogativas especiais, em face da sua maior gravidade e alarme social que provocam ao colocarem em causa valores fundamentais da comunidade[6], tais como, entre outras: a proteção das testemunhas e de outros intervenientes no processo contra formas de ameaça, pressão ou intimidação (artigo 139.º); realização de buscas domiciliárias ordenadas ou autorizadas pelo juiz, entre as 21 e as 7 horas (artigo 177.º, n.º 1 e 2, al. a)); admissibilidade de interceções telefónicas (artigo 187.º, n.º 2, al. a)); imposição ao arguido de medida de

[5] Artigo 1.º, al. m) do Código de Processo Penal.
[6] Cf. Preâmbulo da Lei n.º 58/2020, de 31 de agosto, que atualizou o Código Penal em vigor.

coação de prisão preventiva (artigo 202.º, n.º 1, al. c)); elevação nos prazos de duração máxima de prisão preventiva a que o arguido pode ser sujeito (artigo 215.º, n.º 2).

Embora a gravidade de todos os crimes que se inscrevem na tipologia "criminalidade altamente organizada", importa relevar com especial acuidade as condutas em que exista uma "associação criminosa"[7] vista como uma organização de "crime organizado", onde se verifica uma estrutura desenvolvida, uma hierarquia e estabilidade organizativa temporal, como que de uma empresa se tratasse (Anes, 2015), mas cuja atividade desenvolvida provenha ou tenha ligação a países externos a Portugal e que preencham o tipo de criminalidade que denominamos de "criminalidade organizada transnacional", considerando a internacionalização do crime perpetrado, em que se assiste a uma grande flexibilidade geográfica através da ação organizada de diversos indivíduos estrangeiros com ligações transnacionais definidas[8].

Efetivamente, em aproveitamento de um mercado global e da livre circulação de pessoas e bens, grupos organizados de criminosos gozam de formação em técnicas específicas, com organização e planeamento de crimes nos países de origem, em que *a posteriori* e munidos de uma "carta de missão" vêm a executar atividades criminosas em vários países da Europa, a que Portugal não é exceção, visando naturalmente o máximo lucro.

Tendo em conta este quadro, cumpre-nos questionar, desde logo, se as autoridades com responsabilidade nacionais e internacionais, tendo em conta os meios à sua disposição, têm sido eficientes na prevenção e combate à criminalidade organizada transnacional que assola os diversos países da UE, agora que se verifica não só o esbater de fronteiras físicas, por força da aplicação do acordo Schengen, mas também o derrube de fronteiras tecnológicas, a que o crime organizado não deixa de aproveitar, conquanto os

[7] Sem nos determos especificamente na definição do conceito de "associação criminosa", importa referir que o crime de associação criminosa exige a congregação de três elementos essenciais: um elemento organizativo, um elemento de estabilidade associativa e um elemento de finalidade criminosa, conforme Acórdão do TRP 01.12.2017, obtido de http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/a9b57564fd92e3e980258218005302bc?OpenDocument.

[8] Nos termos da Convenção das Nações Unidas Contra a Criminalidade Organizada (Convenção de Palermo), nomeadamente artigo 3.º, n.º 2 al. a) que refere que o crime é transnacional se cometido em mais do que um Estado.

lucros provenientes do tráfico de estupefacientes "são de tal forma elevados e significativos (…) permitindo, direta ou indiretamente, ao crime organizado, ter um peso significativo nos centros de decisão económica" (Braz, 2004, p. 175) podendo, seguramente se afirmar, que a maioria da criminalidade organizada hodierna não vive sem o crime de tráfico de estupefacientes associado às suas atividades ilícitas.

1.2 – Criminalidade organizada. O Espaço Schengen

Em face da globalização que cada vez mais se assiste a nível internacional, nomeadamente através das diversas alterações que se têm verificado a vários níveis tais como geográficas, culturais, políticas e sociais, impele-nos a olhar com grande preocupação para os fenómenos criminais oportunistas que daí advêm, particularmente para a criminalidade organizada, em face do impacto que este tipo de crime tem na sociedade e no sentimento de insegurança que provoca nas populações, importando identificar qual ou quais as melhores formas de a prevenir e combater, contando com a sua patente complexidade e globalidade (Prates, 2011).

De facto, no que concerne à criminalidade organizada, assiste-se hoje a uma grande flexibilidade geográfica através da ação organizada de diversos indivíduos, estrangeiros com ligações transnacionais definidas (Prates, 2011), exigindo-se um suplementar e extraordinário esforço das forças e serviços de segurança na identificação, prevenção e combate a essas novas formas de criminalidade.

Por força da "aldeia global" em que vivemos também o crime se tornou global, podendo hoje se falar na cosmopolitização do crime porquanto temos assistido a vagas de crime perpetrado por grupos organizados itinerantes que, em face da fácil mobilidade pelo menos dentro do espaço Schengen, se deslocam aos diferentes países cometendo diversos crimes, nomeadamente crimes contra pessoas e contra o património, de forma planeada e organizada.

Como anteriormente demos nota, existem diversos grupos criminosos organizados com proveniência de países externos, tanto de países fora da UE como de países de contexto europeu, que desenvolvem a sua atividade criminal em território nacional, sustentados numa organização que perpassa

várias fronteiras, denotando-se grande flexibilidade na atuação destes grupos criminosos, tanto ao nível de diferentes *modi operandi* como ao nível da atuação através de diversas tipologias criminais.

Na senda do defendido por Luís Elias, a pulverização global do crime deve-se, entre várias razões, à abolição de fronteiras no espaço Schengen, que veio permitir uma maior movimentação de pessoas e de bens, mas também de criminosos internacionais, com um controlo fronteiriço ineficaz (Elias, 2018).

Assim, pode-se afirmar que por força da facilitada movimentação de pessoas, adveniente da globalização, que veio permitir que os grupos organizados de criminosos aproveitassem as zonas de comércio livre e a redução de controlo de fronteiras em alguns países do mundo, emergiram mercados lucrativos onde, por força da falha de atuação e controlo policial (Rodrigues, 2009), as organizações criminosas não deixaram de aproveitar essas facilidade para perpetrar crimes, minimizando a possibilidade de serem detidos e/ou responsabilizados *a posteriori*, potenciando o crime sem castigo.

Com o acordo Schengen, assinado em 14 de junho 1985 pela Alemanha, a Bélgica, a França, o Luxemburgo e os Países Baixos, repristinando algumas ideias míticas do passado e que serviram de base da ideia inicial de unidade europeia (Campos & Campos, 2010) e que visou "suprimir gradualmente os controlos nas fronteiras internas e instaurar um regime de livre circulação para todos os nacionais dos países signatários, dos outros países da União Europeia (UE) ou de certos países não pertencentes à UE"[9] e, depois, com a Convenção de Aplicação do Acordo Schengen (CAAS), com a densificação e regulamentação do quadro de condições e garantias de criação de um espaço sem controlo de fronteiras internas entre os países aderentes, assinada em 19 de junho de 1990 e com entrada em vigor em 1995, Portugal passou a ser membro do Espaço Schengen[10], sendo que a liberdade de circulação de pessoas dentro deste espaço passou a fazer parte natural da vida dos cidadãos dos países signatários.

[9] Acordo e Convenção de Schengen. (sem data). Obtido de https://eur-lex.europa.eu/summary/glossary/schengen_agreement.html?locale=pt.

[10] Portugal. Panorâmica. (sem data). Obtido de https://europa.eu/european-union/about-eu/countries/member-countries/portugal_pt.

Não obstante os benefícios económicos e sociais advenientes da livre circulação de pessoas dentro do espaço Schengen, e sem prejuízo da implementação de medidas de segurança compensatórias, de carácter vinculativo a todas as entidades com responsabilidades na prevenção e combate da criminalidade e manutenção da ordem pública, com o objetivo de pelo menos se manter os níveis desejáveis de segurança e ordem pública nos diversos Estados[11], a livre circulação de pessoas e bens veio permitir fluxos migratórios e itinerância de grupos criminais, cuja atividade advém de vários países do mundo, mas que se expande nos diversos países da UE, atividades essas a que devemos dedicar a nossa maior atenção.

Uma das várias medidas compensatórias adotadas e que merece maior destaque pela sua importância foi a adoção do Sistema de Informação Schengen II (SIS II)[12] de carácter obrigatório e sem admissão de reservas pelos Estados integrantes que, através de inserção e partilha de dados policiais entre os países do espaço Schengen, visa[13]:

- Controlos policiais e de fronteiras
- Intercâmbio de informação
- Emissão de vistos e autorizações de residência
- Prevenção da criminalidade e instauração de ações penais pela sua prática

Sem querermos desconsiderar todas as medidas compensatórias adotadas certo é que os grupos de criminosos itinerantes continuam a atuar em países terceiros, de forma organizada, aproveitando brechas legislativas, corredores transfronteiriços e oportunidades ilícitas no "mercado global" em ordem a maximizar lucros ilicitamente obtidos (Davin, 2007).

[11] Materializadas através da Convenção de Aplicação do Acordo de Schengen (CAAS) e regulamentada pelo Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006 (Código de Fronteiras) e pelo Regulamento (CE) n.º 810/2009, do Parlamento Europeu e do Conselho, de 13 de julho de 2009.
[12] Artigo 1.º da Decisão 2007/533/JAI do Conselho, de 12 de junho e Regulamento 1987/2006 do Parlamento e do Conselho (Regulamento SIS II).
[13] Sistema de Informação de Schengen de segunda geração. (2020, 28 de dezembro). Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14544.

1.3 – Criminalidade organizada e cibercriminalidade. Tendências

Como referimos anteriormente a criminalidade organizada, após a abertura das fronteiras derivada do acordo Schengen, expandiu-se de forma tentacular, continuando atualmente a "representar uma ameaça à segurança global, com impactos diretos nos cidadãos – e nos seus direitos, liberdades e garantias –, bem como ao desenvolvimento económico e à estabilidade de instituições e países" (RASI, 2021, p. 31), agora principalmente por força do desenvolvimento das novas tecnologias de informação que vieram derrubar as fronteiras tecnológicas do crime.

A criminalidade organizada hodierna não conhece barreiras físicas nem tecnológicas, "quer pela sua transnacionalidade, quer pelo modelo que as tecnologias disponíveis e os fluxos migratórios permitem estruturar" (Santos, 2015, p. 136), sendo que "a internet e as redes digitais em geral constituem-se (…) como um novo ambiente para a criminalidade organizada" (Elias, 2018, p. 302).

A Internet, efetivamente, garante um nível de comunicação entre os membros dos grupos organizados de criminosos, difícil de deter pelas autoridades competentes para a investigação de crimes, tanto pelo nível de encriptação das comunicações, como pelo facto de haver uma utilização massificada pelos criminosos, no âmbito da sua atuação, de dispositivos tecnológicos descartáveis, dificultando a atuação das autoridades policiais ou judiciárias que "se confrontam com mudanças sucessivas e inesperadas de equipamentos e até de operadoras" (Davin, 2007, p. 43).

Segundo o RASI de 2021, os crimes informáticos, que integram as tipologias de acesso indevido ou ilegítimo, interceção ilegítima, falsidade informática, sabotagem informática, viciação ou destruição de dados, dano relativo a programas, reprodução ilegítima de programa protegido, e outros crimes informáticos, em termos percentuais diminuíram 10,5% (p. 62), não obstante ter sido reconhecido pelo mesmo relatório:

> o risco de crimes informáticos ou praticados por meio informático, pela elevada utilização de aquisições/investimentos por pessoas com

> insuficiente literacia tecnológica e financeira através de plataformas/sites na Internet, e pela segurança/anonimato de utilização da deep web e/ou *dark web*, nomeadamente para compra/venda de moeda e branqueamento (RASI, 2021, p. 70).

Por seu turno, também como indicador importante, a nota informativa, de 13 de julho de 2022, do Gabinete de cibercrime da Procuradoria-geral da República relativo às denúncias de cibercrime recebidas, eletronicamente, no 1.º semestre de 2022[14], informa que foram recebidas 852 queixas, mais 258 do que em período homólogo em 2021[15], e mais 547 do que no mesmo período de 2020, o que demonstra, uma subida considerável e consistente de ano após a ano.

De facto, segundo o Internet Organised Crime Threat Assessment de 2021 (IOCTA, 2021), relatório estratégico sobre as principais ameaças emergentes e desenvolvimentos no cibercrime, publicado anualmente pelo *European Cybercrime Centre* (EC3) da EUROPOL, os utilizadores da *dark web* utilizam, cada vez mais, aplicativos como o Wickr[16] e o Telegram[17] como canais de comunicação de modo a garantir o anonimato das suas comunicações, bem como adotam cada vez mais criptomoedas anónimas, como a Monero[18].

Ainda segundo o IOCTA de 2021, em face dessa utilização anónima, os grupos organizados de criminosos têm aumentado a sua atividade, bem como melhorado a sua segurança operacional para proteger os seus lucros

[14] Cibercrime em 2022 (1.º semestre) – Denúncias recebidas. (2022, 13 de julho). Obtido de https://cibercrime.ministeriopublico.pt/pagina/cibercrime-em-2022-1o-semestre-denuncias-recebidas, onde se descrevem as denúncias de cibercrime, recebidas pelo Gabinete Cibercrime, por correio eletrónico, no primeiro semestre de 2022. Segundo informação referida na referida página *online*, as denúncias descritas "são um indicador real da cibercriminalidade de que são vítimas os portugueses, embora, naturalmente, não possam dar origem a dados estatísticos rigorosos".

[15] O que representa um aumento de 143%, entre períodos homólogos.

[16] "Aplicativo para Android e iPhone designado para ajudar as pessoas no envio de mensagens, incluindo fotos e anexos, que são automaticamente eliminados a partir de determinado lapso temporal" (Wikipédia, 2022).

[17] "Serviço de mensagens instantâneas baseado na nuvem. O telegram está disponível para smartphones ou tablets (Android, iOS, Windows Phone, Ubuntu touch, Firefox OS), computadores (Windwos, OS X, GNU/Linux) e também como aplicação WEB" (Wikipédia, 2022).

[18] Criptomoeda de código aberto, "criada em abril de 2014, cujo enfoque se baseia na privacidade, não rastreabilidade e na descentralização, com diversas carteiras disponíveis para Windows, macOS, iOS, Linux, Android e FreeBSD" (Wikipédia, 2022).

proveniente das suas atividades ilícitas (p. 9), sendo que desde o início da pandemia Covid-19, os cibercriminosos têm aproveitado o facto de as empresas terem recorrido massivamente a teletrabalho e, por tal razão, terem se tornado mais descuidadas com as políticas de segurança de tecnologias de informação, registando-se um aumento de vulnerabilidades e ataques através da internet visível ou de superfície (p. 20).

Quanto à *dark web*, o supra relatório refere que as autoridades judiciárias dos Estados da UE não têm acompanhado o cenário de ameaças, o que releva para efeitos de consolidação dos desenvolvimentos que já tinham ocorrido há alguns anos (p. 36), verificando-se um aumento de criminalidade através do *crime-as-a-service* nos mercados da *dark web*, bem como melhorias na segurança operacional dos grupos organizados de criminosos, que usam e aproveitam-se da comunicação criptografada de *end-to-end* (p. 6).

Segundo Elias "os *modi operandi* utilizados pelos piratas informáticos apontam para a transversalidade e transdisciplinaridade dos crimes" (Elias, 2018, p. 341), o que significa dizer que as tendências criminais atuais, dos grupos organizados de criminosos, são no sentido de abarcar uma multiplicidade de crimes, em simultâneo, potenciadas pelas novas tecnologias, ao seu serviço.

Como se depreende a cibercriminalidade é uma ameaça real e global, que opera tanto ao nível da internet de superfície, como ao nível da *dark web*, atingindo todos os Estados membros da UE cujas fronteiras tecnológicas são desconhecidas dos grupos organizados de criminosos, que desenvolvem a sua atividade ilícita fluidamente no espaço cibernético, potenciando trocas comerciais ilegais, dificilmente rastreáveis e detetáveis, o que dificulta a ação das autoridades competentes na matéria.

1.4 – A internet como motor da criminalidade organizada

Na sequência dos objetivos, de caráter programáticos, delineados pelo Governo de Portugal no seu programa de Governo 2019-2023, considerando que a segurança é um pilar fundamental do Estado de Direito Democrático e um garante da liberdade dos cidadãos, também neste documento vem demonstrada a preocupação com diversos fenómenos, onde consta o tráfico de

droga e o cibercrime como "fenómenos criminais de crescente complexidade que reclamam respostas atualizadas e mais eficazes"[19].

De acordo com o Relatório Anual de Segurança Interna relativo ao ano de 2020 (RASI, 2020), a situação pandémica e as medidas de contingência implementadas introduziram perturbações muito significativas nos circuitos e nas dinâmicas do tráfico ilícito de estupefacientes, levando por isso a quebras significativas, com exceção no tráfico por via marítima, fazendo com que as organizações criminosas se adaptassem a esta nova realidade, utilizando novos *modi operandi* – mercados *online*, plataformas digitais, redes sociais e serviços de entrega rápida.

Não obstante o referido, independentemente da situação pandémica vivenciada, tem-se verificado nos últimos anos um aumento de cibercriminalidade e de exploração de comércio *online*, relevando para tanto a utilização de dispositivos eletrónicos inteligentes, o que abrange telefones, telemóveis e outros dispositivos que se liguem em rede, que não computadores (Verdelho, 2006), utilização da internet e vulgarização do uso das redes sociais que revestem, no que concerne à utilização da internet lícita, um "veículo" propulsor de aproveitamento das organização criminosas (Elias, 2011), posição esta que é corroborada pelo RASI, ao afirmar que, de facto, o comércio *online*, representa "oportunidades para os mercados criminais que poderão ter implicações de longo-prazo na sua expansão", perspetivando-se que no futuro próximo se multiplique novos universos de cibercrime (RASI, 2020).

Efetivamente, é de recordar que há mais de 20 anos que as Autoridades Nacionais verificaram o surgimento de "novos desafios para o controlo do circuito das drogas, como a divulgação da conceção e a comercialização de drogas ilícitas por computador, via internet"[20], considerando que o processo de

[19] Programa do XXII Governo Constitucional, 2019-2023. (sem data). Obtido de https://www.portugal.gov.pt/gc22/programa-do-governo-xxii/programa-do-governo-xxii-pdf.aspx?v=%C2%ABmlkvi%C2%BB=54f1146c-05ee-4f3a-be5c-b10f524d8cec.

[20] Estratégia Nacional de Luta contra a Droga (ENLCD), aprovada pela Resolução do Conselho de Ministros n.º 46/99, de 26 de maio. Obtido de http://www.sicad.pt/BK/Publicacoes/Lists/SICAD_PUBLICACOES/Attachments/71/ENresolucao.pdf.

globalização veio permitir uma sofisticação de processos com utilização da internet como veículo para a produção e comercialização de drogas ilícitas[21].

O Plano Nacional para a redução dos comportamentos aditivos e das dependências, 2013-2020 (PNRCAD 2013-2020) viria, igualmente, a demonstrar essa preocupação através da estratégia delineada, referindo-se à necessidade de regulamentação e harmonização legal de modo a garantir a redução da oferta e diminuição da disponibilidade e do acesso às substâncias ilícitas tradicionais e às novas substâncias psicoativas através da internet[22], mas que, parece-nos, ainda de forma tímida, visto que ao nível operacional não se vieram a concretizar medidas substantivas e concretas para a redução da oferta de substâncias ilícitas através da internet, paradigma que desejamos que se altere no novo Plano em discussão para os próximos anos (2021-2030).

O Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências (SICAD) ao longo dos últimos anos tem, igualmente, vindo a chamar à atenção para o fato de que no domínio da oferta "vários indicadores apontam para uma maior circulação de drogas no mercado nacional numa conjuntura de grandes desafios, como o crescente uso da internet na comercialização de diversas substâncias psicoativas", concluindo através do IV Inquérito nacional ao consumo de substâncias psicoativas na população geral (INPG) – 2016/17 que, ao nível da perceção da facilidade de acesso na obtenção de drogas, em todas as faixas etárias de consumidores, mais de 50% considera fácil/muito fácil obtenção, e que mais de 40% da população consumidora de novas substâncias psicoativas afirmou que as obteve através da internet[23].

[21] Sobre estas tendências referenciadas na ENLCD é de mencionar que as mesmas tiveram como suporte o *Report of the International Narcotics Control Board* for 1998, OICE, Nações Unidas, Nova Iorque, 1999.

[22] Plano Nacional para a redução dos comportamentos aditivos e das dependências. (2013-2020). (2013). Obtido de http://www.sicad.pt/BK/Institucional/Coordenacao/Documents/Planos/SICAD_Plano_Nacional_Reducao_CAD_2013-2020.pdf.

[23] Relatório Anual 2019. A situação do País em Matéria de Drogas e Toxicodependências (SICAD, 2019). (2020). Obtido de http://www.sicad.pt/BK/Publicacoes/Lists/SICAD_PUBLICACOES/Attachments/169/Relatorio_Anual_2019_A_SituacaoDoPaisEmMateriaDeDrogas_e_Toxicodependencias.pdf.

A nível europeu, no que concerne aos mercados de droga através da *darknet*, foi igualmente referido em 2017 no Relatório[24] conjunto elaborado pela EMCDDA[25] e pela EUROPOL[26], que o mercado de tráfico de drogas através da *darknet* representou, entre 2011-2015, cerca de 46% da totalidade de vendas.

De facto, a evolução tecnológica marcou – e continua a marcar – indelevelmente muitos aspetos da vida quotidiana, incluindo a forma como os bens ilícitos são comercializados.

O referido relatório conclui, igualmente, que o mercado *online* ou "cryptomarkets" está em franca expansão e permite que vendedores e compradores efetuem transações *online* sem divulgarem os seus detalhes, garantindo assim um grau de anonimato considerável, facto este que nos leva a reconhecer que a proliferação do comércio de bens ilícitos *online* é uma área crítica de sucesso para as atividades desenvolvidas por grupos de criminosos organizados na União Europeia.

Em termos de conclusões, o Relatório que nos vimos a referir, e considerando as dificuldades de recolha de dados nesta área de atividade, como, pensamos, temos vindo a demonstrar, projeta como de extrema relevância várias recomendações, as quais destacamos as seguintes:

i. Maior consciencialização para o problema: pois de facto o desenvolvimento das tecnologias de informação estão patentes em vários aspetos da vida moderna, onde se incluí o *modus operandi* de como são comercializados produtos ilícitos pelos grupos organizados de criminosos, pelo que o policiamento do uso de plataformas de internet pelos criminosos deve ser uma prioridade nos países da UE, admitindo no entanto as dificuldades inerentes ao desmantelamento das redes criminosas que operam de forma muito resiliente na *darknet* considerando que compradores e vendedores rapidamente passam de plataforma em plataforma, de modo a não serem descobertos, pelo que a abordagem tem de ser integrada e as

[24] European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), *Drugs and the darknet: Perspectives for enforcement, research and policy*, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg. Obtido de https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet_en.
[25] European Monitoring Centre for Drugs and Drug Addiction.
[26] European Union's law enforcement agency.

medidas a implementar, para serem mais efetivas, têm de considerar toda a cadeia de produção de droga, desde os produtores, passando pelos percursores e pequenos traficantes, até aos cabecilhas das redes organizadas de criminosos;

ii. Coordenação nacional e cooperação internacional: alocar recursos específicos e dedicados ao problema, como por exemplo criar unidades de combate ao crime praticado através da *darknet*, juntando especialistas de investigações criminais na área das tecnologias de informação com especialistas de investigação no tráfico de droga. Tendo em consideração que por norma os mercados ilícitos *online* não operam apenas perante uma localização que abranja um só Estado, torna-se importante criar equipas de investigação conjuntas e ações coordenadas a nível europeu, tais como ciber patrulhas[27];

iii. Cooperação com entidades privadas: colaboração e cooperação próxima com entidades privadas, tais como empresas de tecnologias de informação, redes sociais, serviços de pagamento *online* e empresas de distribuição revela-se de extrema importância, contando que ambas as partes têm interesse em identificar novas ameaças e dar resposta rápida às mesmas, tendo as empresas privadas muitas das vezes tecnologia de ponta e *know how* altamente desenvolvido não disponibilizada às autoridades públicas.

Por seu turno, o Relatório Europeu sobre Drogas. Tendências e evoluções, 2021 (RED, 2021)[28], que nos oferece um panorama rico acerca da produção, o tráfico, a distribuição e o consumo de drogas na Europa, também

[27] De facto é de mencionar (e de louvar) as operações de *Cyber-Patrolling Week*, da iniciativa da EUROPOL, que têm ocorrido desde 2017, operações que contam com diversos participantes dos países Estados-membros da UE (coordenados pelo *European Cybercrime Centre (EC3)*) e que visam o combate da criminalidade em evolução na darknet, em diversas áreas, mormente o tráfico de produtos estupefacientes. Em face da mais-valia e sucesso declarado deste tipo de ações operacionais concertadas, a EUROPOL, no seu Plano de Atividades para 2021-2023 prevê nas suas atividades operacionais a desenvolver operações de cyber patrolling e ações contra mercados da *dark web*. Disponível em https://www.europol.europa.eu/publications-documents/europol-programming-document.

[28] Observatório Europeu da Droga e da Toxicodependência (2021), Relatório Europeu sobre Drogas 2021: Tendências e Evoluções, Serviço das Publicações da União Europeia, Luxemburgo. Obtido de https://www.emcdda.europa.eu/system/files/publications/13838/2021.2256_PT_03.pdf.

nos informa, desde logo, que a pandemia não afetou seriamente a disponibilidade de drogas na Europa, continuando-se a verificar riscos graves para a saúde pública derivados da "disponibilidade [e disponibilização] e utilização de uma vasta gama de substâncias, muitas vezes de elevada potência e pureza" (RED, 2021).

Essa disponibilização de drogas efetua-se, cada vez mais, através da utilização de serviços de mensagens encriptadas, aplicações nas redes sociais, fontes *online* e serviços de correio e distribuição ao domicílio, levando-nos a afirmar da possibilidade de que a pandemia tenha vindo reforçar a capacidade digital dos mercados de droga (RED, 2021), considerando que os traficantes resiliente e rapidamente se adaptaram às restrições derivadas do encerramento de fronteiras físicas.

Na mesma sequência, também o Relatório anualmente desenvolvido pela Europol relativo à avaliação das ameaças graves e do crime organizado, SOCTA[29], veio em 2021, revelar o crescimento do cibercrime, em diversas áreas como abuso sexual de crianças, contrabando de tabaco, tráfico de estupefacientes (definido como a principal atividade das redes criminosas), imigração ilegal e corrupção – sendo esta última de tal forma especialmente preocupante que é tido como uma das ameaças mais preocupantes nos próximos anos – são os motores do crime organizado.

Neste patamar, a Estratégia da UE de Luta conta a Droga (2021-2025)[30], aprovada pelo Conselho da Europa veio definir o quadro político e as prioridades da política da UE de luta contra a droga para o período 2021-2025, reforçando a ideia de que deve ser tido como prioritário, no domínio da oferta de droga/reforço da segurança, agir de forma estratégica e reforçada quanto à evolução dos mercados europeus de droga, quanto à utilização de plataformas *online*, aplicações móveis, redes sociais, e internet (surface web e darknet) para o tráfico de produtos estupefacientes, pois "estas tendências não se atenuaram durante a crise do COVID-19, bem pelo contrário" (Estratégia…, 2021-2025).

[29] European Union Serious and Organised Crime Threat Assessment 2017. (2021, 6 de dezembro). Obtido de https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

[30] Aprovada pelo Conselho em 18 de dezembro de 2020. Obtido de https://www.consilium.europa.eu/pt/press/press-releases/2020/12/18/council-approves-the-eu-drugs-strategy-for-2021-2025/.

De relevar que a Estratégia […], (2021-2025), que se baseou nos ensinamentos das estratégias anteriores da UE de luta contra a droga e respetivos planos de ação, bem como na avaliação contínua da situação atual em matéria de droga efetuadas pelo Observatório Europeu da Droga e da Toxicodependência (OEDT) e pela EUROPOL, teve igualmente em conta a Estratégia da UE para a União da Segurança para 2020-2025[31], que também define como vetor prioritário, a desenvolver ao longo dos cinco anos definidos, o reforço da cibersegurança para que se possa antecipar a evolução das ameaças e fazer-lhes face, considerando que a luta contra a cibercriminalidade deve tornar-se uma prioridade estratégica da comunicação em toda a UE, pois "combater a cibercriminalidade significa olhar para o futuro".

Por último, de relevante importância importa evidenciar o Plano de Ação da União Europeia em matéria de drogas 2021-2025[32], que vem concretizar a Estratégia anteriormente aprovada, e que assenta em três pilares essenciais com o objetivo de reduzir a oferta da droga no seio da UE: reforço da segurança, redução da procura de droga (aposta nos serviços de prevenção, tratamento e prestação de cuidados), bem como enfrentar os danos relacionados com a droga, pilares esses que importam ser concatenados com os vetores da cooperação internacional, investigação, inovação, prospetiva e coordenação, governação e execução, que devem servir de apoio aos domínios de intervenção que revestem os pilares fundamentais considerados[33].

Assim, no âmbito da prioridade estratégica n.º 3, o Plano assume como prioritário travar os mercados de drogas ilícitas de base digital, definindo-se como Ação concreta "acompanhar os mercados de droga na internet visível e oculta executando a ação preparatória proposta pelo Parlamento Europeu de monitorização permanente da Internet obscura a fim de garantir resultados abrangentes"[34], assinalando como indicador dos mercados de droga (fontes

---

[31] Documento 52020DC0605. (sem data). Obtido de https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

[32] Aprovado no dia 21 de junho de 2021, sob a presidência portuguesa do Conselho da União Europeia. Obtido de http://www.sicad.min-saude.pt/pt/Paginas/detalhe.aspx?itemId=560&lista=SICAD_NOVIDADES&bkUrl=/BK.

[33] *Idem.*

[34] * Para mais pormenores, consultar o número 18 02 77 04 – Ação preparatória – Monitorização coordenada da Internet obscura pela UE para combater atividades criminosas, na página 61 do anexo 3 das observações orçamentais dos projetos-piloto e ações preparatórias.

estatísticas e outras fontes habituais de informação), entre outros, as tendências e evolução da utilização da internet obscura e de outros meios facilitados pelas tecnologias digitais para venda de drogas[35].

Em suma, consideramos que estes importantíssimos relatórios, nacionais e europeus têm um denominador comum: a preocupação na luta contra o tráfico de estupefacientes, em especial, o cometido através de tecnologias de informação e plataformas *online* que, como dito, configuram os "motores do crime organizado", que urge combater.

1.5 – Conclusão capitular

Se a globalização veio aproximar os povos e garantir o desenvolvimento económico, social e cultural entre os Estados, potenciada pela inserção tecnológica, onde o conhecimento é veiculado à distância de um clique, através do ciberespaço, criando aquilo que hoje denominamos de "Global Common", certo é que essas transmutações, conjugadas com as fronteiras abertas no espaço Schengen, no que concerne aos Estados integrantes, vieram, também, dar corpo e consolidar novas tendências criminais, permitindo uma maior itinerância da criminalidade organizada transnacional.

Em face da sua complexidade e dificuldade de deteção, a criminalidade organizada transnacional tem prosperado, operando a partir de diversos países incidindo em outros, com benefícios altamente remuneratórios para os criminosos, exigindo-se um esforço suplementar por parte das autoridades policiais na sua prevenção e combate, sem prejuízo das medidas de segurança compensatórias existentes no espaço Schengen, que procuram garantir a manutenção dos níveis de segurança e ordem pública nos diversos Estados integrantes.

Considerando o desenvolvimento das novas tecnologias de informação, que veio incrementar o âmbito de atuação dos grupos organizados de criminosos, reconhecido nacional (RASI) e internacionalmente (IOCTA), que lhes permite operar através de canais de comunicação que garantem o anonimato e confidencialidade da sua atividade criminal (Ramos, 2022), urge desenvolver políticas de segurança tecnológicas, por parte das autoridades

[35] *Idem ibidem*.

competentes, que permitam minimizar as vulnerabilidades expostas e recorrentemente aproveitadas pelos grupos organizados de criminosos, colocando em causa a segurança operacional desses grupos.

De facto, os cibercriminosos utilizam os sistemas informáticos para praticar crimes e, igualmente, para suprimir as provas da sua prática, dificultando as investigações criminais, pois os meios investigatórios à disposição dos OPC são, ainda muito vocacionados para recolha de "provas corpóreas", sendo insuficientes e desadaptados para dar uma resposta eficiente e eficaz à cibercriminalidade (Nunes, 2021).

Relativamente ao crime de tráfico de estupefacientes através da internet, enquanto crime crescentemente cibernético, de progressiva complexidade, impõe-se necessário harmonizar a legislação atualmente em vigor, de modo a vir-se a reduzir a oferta e disponibilidade de acesso a substâncias estupefacientes na internet, considerando a facilidade de obtenção de substâncias psicoativas através do ciberespaço, sendo que os dados disponíveis, retirados do IV inquérito nacional ao consumo de substâncias psicoativas na população geral (2016/2017) indicam que mais de 40% dos consumidores obteve essas substâncias através da internet.

Em face do paradigma enunciado, urge aos Estados, através da Autoridades com competência na investigação criminal, garantir o policiamento do uso, por parte de grupos organizados de criminosos, de plataformas *online*, alocando recursos específicos e dedicados ao problema, em coordenação com autoridades europeias dedicadas (Cyber-patrolling – Europol e EC3), bem como aumentar a cooperação com entidades privadas, como empresas de serviço de pagamento *online* e redes sociais, de modo a sustar a franca expansão do tráfico de estupefacientes através da internet e de meios de comunicação *online*, como conclui o Relatório do OEDT (2017).

CAPÍTULO 2

COORDENAÇÃO E COOPERAÇÃO INTERNACIONAL

2.1 – Cooperação policial internacional

Como referimos anteriormente, por força do derrube das fronteiras físicas e tecnológicas, assistimos o que Braz denomina de "internacionalização do fenómeno do tráfico ilícito de drogas" (Braz, 2004, p. 175), urgindo capacitar os Estados de novos entendimentos e colaboração mútua, relevando a necessidade de uma cooperação internacional policial eficiente e eficaz.

A cooperação policial internacional efetuada entre as diversas polícias de vários países do Mundo, mediada através de Agências internacionais e europeias de cariz policial, tem-se relevado fundamental na prevenção e combate da criminalidade organizada transnacional, porquanto através dos canais instituídos permitem um rápido intercâmbio e partilha de informações criminais relevantes sobre a caracterização de grupos de criminosos e os seus *modi operandi*, possibilitando que as autoridades policiais ajam com maior eficiência na sua deteção e desmantelamento, pois, e acompanhando Luís Elias:

> em face da transnacionalidade do crime, hoje é crucial a troca de informações e a cooperação internacional entre as Polícias e as autoridades judiciárias para conseguir combater no exterior as ameaças e riscos que possam ter uma repercussão na segurança interna (Elias, 2018, p. 109).

Existe um grande enfoque das Agências e Entidades com responsabilidades no que concerne à criminalidade organizada transnacional que tem feito com que, para a identificação de um conjunto alargado de crimes que os grupos organizados de criminosos (OCG) desenvolvem, bem como para a consequente caracterização dos seus *modi operandi*, exista uma necessidade de troca de informações fluída entre os países envolvidos e as

diversas agências que objetivam a prevenção e o combate do crime organizado não só no seio dos Estados-Membros da EU, como a nível internacional.

Das Agências com maior relevância nesse comprometimento, com grande envolvimento através dos canais de cooperação instituídos nos Estados abrangidos, importa destacar a EUROPOL, a INTERPOL e os GABINETES NACIONAIS SIRENE.

A EUROPOL[36] é um serviço europeu de polícia, que foi criado em 1 de outubro de 1998, cuja principal responsabilidade passa pelo tratamento e intercâmbio de informação criminal, principalmente no âmbito da prevenção e combate à criminalidade organizada.

Encontra-se sediada em Haia, nos Países Baixos, e presta apoio aos 27 Estados-Membros da UE, colaborando ainda com diversos países terceiros e outras organizações internacionais com propósitos idênticos, operando através de um centro de apoio às operações policiais, de um centro de competências em matéria de aplicação da lei, contando com uma plataforma de informações sobre atividades criminosas[37], sendo-lhes permitido o acesso de dados e informações policiais de congéneres de outros Estados-Membros, nos termos da sua regulamentação[38].

Esta Agência tem como objetivo principal apoiar e reforçar a ação das autoridades competentes dos Estados-Membros e a sua cooperação mútua em matéria de prevenção e luta contra a criminalidade grave que afete dois ou mais Estados-Membros, o terrorismo e formas de criminalidade que afetem um interesse comum abrangido pela política da União[39], incumbindo-lhe coordenar, organizar e realizar investigações e ações operacionais (OAP) a fim de apoiar e reforçar a ação das autoridades competentes nos Estados-Membros em que são conduzidas, fornecer informações e apoio analítico aos Estados-membros em ligação com acontecimentos internacionais importantes, e a recolha,

[36] https://www.europol.europa.eu/pt/about-europol.
[37] *Idem*.
[38] Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0794.
[39] Artigo 3.º do Regulamento (EU) 2016/794.

análise, tratamento e partilha de informação criminal, entre os Estados-Membros da UE, relativa a organizações criminosas[40].

No que concerne ao crime organizado cometido através do ciberespaço, é importante fazer uma referência ao Centro de Inovação da UE para a segurança interna (EU Innovation Hub for internal security[41]), que tem trabalhado em rede (plataforma comum), composta por representantes das agências europeias e instituições da UE, bem como por Estados-membros da UE, cujo objetivo passa por garantir informação atualizada para apoiar o trabalho das autoridades competentes no combate ao crime dos Estados-membros, nomeadamente fornecendo soluções tecnológicas inovatórias comuns, aumentando sinergias entre as Autoridades competentes[42], que poderia ser encarregado pelas diversas agências que a compõem de desenvolver novas ferramentas para melhorar a prevenção e combate ao crime organizado através da internet, designadamente através da darknet[43].

Uma das ferramentas adiantada pelo OEDT, no 2.º evento anual do Centro de Inovação da UE para a segurança interna, consiste na aplicação da inteligência artificial a dados recolhidos de amostras de resina de cannabis, para depois conseguir classifica-los como provenientes da Europa ou de Marrocos, com a virtualidade de facilitar a monitorização internacional de drogas nos mercados europeus de drogas[44], ferramenta que, em face da sua utilização inovadora, poderia vir a ser aplicada a outros contextos e controlo de outras substâncias estupefacientes[45].

Em face das dificuldades de investigação de crimes praticados no ciberespaço, de forma a tornar o trabalho das Autoridades competentes mais eficiente, a Europol Innovation Lab criou o Europol Tool Repository que contém diversas ferramentas de *software* gratuitas, não comerciais, com o objetivo de

---

[40] Conforme previsto no artigo 4.º do citado Regulamento (al. a), c) e e)).
[41] O Centro de Inovação da UE para a segurança interna, foi criado sob as instruções do COSI em 2019, tendo ocorrido a primeira reunião, com atividade virtual, em 2021 (evento anual). Cf. Doc. n.º 12657/22, do Concelho da União Europeia.
[42] https://www.europol.europa.eu/operations-services-innovation/innovation-lab/eu-innovation-hub-for-internal-security#:~:text=The%20EU%20Innovation%20Hub%20for%20Internal%20Security%20is,border%20security%2C%20immigration%2C%20asylum%20and%20law%20enforcement%20practitioners.
[43] Conforme sugerido pela Presidência do Conselho da União Europeia, na nota produzida, em 01 de fevereiro de 2022, em Bruxelas. Doc. n.º 5755/22.
[44] Cf. Relatório do 2.º evento anual do Centro de Inovação da UE para a segurança interna - Anexo ao Doc. n.º 12657/22, do Concelho da União Europeia.
[45] *Idem*.

apoiar os investigadores criminais, como por exemplo o Projeto FREETOOL[46], que desenvolveu uma variedade de ferramentas gratuitas para apoio a investigação de crimes cibernéticos e análises digitais[47].

À INTERPOL[48], que atualmente conta com 195 países membros e se encontra sediada em Lyon, em França, compete-lhe efetuar a cooperação internacional quanto à necessidade de partilha e troca de informações com países terceiros, com vista à prevenção e luta contra a criminalidade através da cooperação reforçada a nível internacional entre as autoridades policiais dos diferentes países membros[49].

Tem como objetivos assegurar a assistência recíproca entre as autoridades de polícia criminal dos países contratantes, no quadro das suas legislações e no espírito da Declaração Universal dos Direitos do Homem, bem como estabelecer e desenvolver todas as instituições capazes de contribuir de forma eficaz para a prevenção e repressão das infrações de direito comum[50].

Conta com um sistema de informações, o I-24/7 INSYST, que lhe permite a comunicação direta de mensagens entre os gabinetes centrais nacionais e o secretariado-geral localizado na sua sede, cuja informação é acessível em tempo real através do sistema, facultando aos países membros o acesso mútuo às respetivas bases de dados nacionais através de um canal específico para o efeito.

Quanto aos dados criminais transmitidos e acedidos pelos países membros, deve o respetivo acesso ser controlado pelos diversos países, dados que devem ser destruídos após acesso nos termos da legislação nacional.

Os gabinetes nacionais SIRENE, existentes em todos os estados contratantes, são responsáveis pela troca de informações suplementares baseadas no Sistema de Informação Schengen (SIS), como por exemplo se uma pessoa é objeto de um controlo e se um procedimento de busca é

---

[46] O FREETOOL é um projeto financiado pela UE (Acordo de Subvenção n.º 821947) que começou em 2012. O objetivo do projeto é atender à necessidade de ferramentas personalizadas para crimes cibernéticos, desenvolvidas por agentes da lei para aplicação da lei. Obtido de https://thefreetoolproject.eu/

[47] *Idem*.

[48] The International Criminal Police Organization, conforme denominado no artigo 1.º da sua Constituição: Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session (Vienna - 1956).

[49] https://www.interpol.int/en/Who-we-are/What-is-INTERPOL.

[50] *Idem*.

iniciado, o sistema apenas revela essa mesma informação (alerta), sendo que qualquer outra informação adicional tem de ser obtida através dos gabinetes SIRENE[51].

Os gabinetes SIRENE nacionais criados pelas partes contratantes da Convenção Schengen são unidades orgânicas do SIS, por onde circulam as informações suplementares dos dados contidos no referido sistema e que são indispensáveis para o cumprimento das ações requeridas aos serviços utilizadores do SIS (forças policiais e outras entidades competentes nos termos da convenção Schengen), sendo responsáveis pela inserção, modificação, retificação e eliminação centralizada das indicações dos respetivos países integrados no SISII[52].

Os dados de interesse possíveis de obter, através das entidades suprarreferidas, passam por, nomeadamente, dados relativos a suspeitos, veículos, armas, documentos, objetos registáveis e *modi operandi* de organizações criminosas de âmbito internacional, de modo a permitir às autoridades policiais nacionais – *in casu* Forças e Serviços de Segurança – prevenir e combater mais eficazmente os delitos criminais perpetrados ou em vias de ser cometidos.

Os canais de cooperação policial internacional constituem, efetivamente, uma enorme mais-valia para as autoridades policiais nacionais ao permitirem um rápido intercâmbio e partilha de informações criminais sobre grupos organizados de criminosos cuja atuação perpassa fronteiras. Para aceder à informação e base de dados destas agências, importa cumprir determinadas regras, tanto nacionais como internacionais, sendo que os países participantes para acederem oportunamente ao manancial de informação criminal, através das forças e serviços de segurança, máxime Órgãos de Polícia Criminal (OPC) competentes, têm de o fazer através dos canais técnicos estabelecidos.

Para beneficiar dos diversos canais de cooperação policial internacionais existentes devem os países obedecer a uma coordenação interna prévia, de acordo com as regras estabelecidas ao nível das agências europeias e

[51] http://euroogle.com/dicionario.asp?definition=880.
[52] Decisão 2007/533/JAI do Conselho, de 12 de Junho de 2007 e Regulamento (CE) N.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de Dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SISII).

internacionais, bem como dentro do quadro regulamentar instituído em cada país[53].

Dentro do quadro regulamentar interno importa, desde já, salientar a Lei n.º 53/2008, de 29/08, Lei de Segurança Interna (LSI), que prevê no n.º 2 do artigo 4.º que "…as forças e serviços de segurança podem atuar fora do espaço referido no número anterior [jurisdição do Estado Português], em cooperação com (…) organizações internacionais de que Portugal faça parte, tendo em vista, em especial, o aprofundamento do espaço de liberdade, segurança e justiça da União Europeia", referindo o n.º 2 artigo 6.º que "…as forças e serviços de segurança cooperam entre si, designadamente através da comunicação de informações que, não interessando apenas à prossecução dos objetivos específicos de cada um deles, sejam necessários à realização das finalidades de outros…".

Por seu turno, a Lei n.º 49/2008, de 27/08, Lei de Organização da Investigação Criminal (LOIC), determina no artigo 10.º que "os Órgãos de Polícia Criminal (OPC) cooperam mutuamente no exercício das suas atribuições", cooperação essa que se fará, nomeadamente, ora através do Sistema integrado de informação criminal (artigo 11.º, n.º 1), ora precisamente através da cooperação internacional (artigo 12.º).

A LOIC especifica que compete à Polícia Judiciária assegurar o funcionamento das Unidades responsáveis pela centralização e tratamento de informação proveniente e a partilhar com a Unidade Nacional Europol (UNE) e com o Gabinete Nacional Interpol (GNI) (artigo 12.º, n.º1), sendo que para assegurar o previsto no n.º 4 do mesmo artigo – acesso a todos os OPC à informação a disponibilizar pela UNE e GNI – necessariamente terá de haver uma coordenação prévia entre os diversos OPC e a PJ, por ser esta a ter a competência de gestão do funcionamento das Unidades nacionais de ligação com a Europol e Interpol[54].

[53] Portugal aprovou, através da Lei n.º 74/2009, de 12/08, o regime aplicável ao intercâmbio de dados e informações de natureza criminal entre as autoridades dos Estados membros da União Europeia, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2006/960/JAI, do Conselho, de 18 de dezembro.

[54] Em Portugal o acesso a informações criminais de suspeitos estrangeiros é efetuado através do Gabinete Nacional Interpol e Unidade Nacional Europol, mediado pela Polícia Judiciária. Neste âmbito, existindo uma entidade criada, em 2017, com competências específicas para a cooperação policial internacional, o Ponto Único de Contato para a Cooperação Policial Internacional, com garantias de maior eficiência e eficácia no tratamento e partilha de

Dito isto, cremos que para haver uma cooperação policial internacional eficaz e eficiente, importante se revela que a montante – ao nível da cooperação e coordenação dentro de cada país – haja uma coordenação interna, entre as forças e serviços de segurança, igualmente eficaz e eficiente que funcione de forma não turbulenta e que contribua para os objetivos comuns, de combate ao crime grave e organizado, em especial o transnacional, pois de facto, na luta contra a criminalidade organizada transnacional, existe uma grande necessidade de troca e partilha de informações entre os países envolvidos e as diversas agências que objetivam a prevenção e o combate do crime organizado e grave, tais como a EUROPOL e a INTERPOL.

2.2 – Canais de Cooperação policial interna

Quanto à necessária coordenação que deve existir entre os OPC, a LOIC prevê o formato de como se deve verificar, nomeadamente nos artigos 13.º a 16.º, destacando-se o Conselho Coordenador dos OPC que é presidido pelos membros do Governo responsáveis pelas áreas da justiça e da administração interna, integrando diversas entidades (Secretário-Geral do Sistema de Segurança Interna (SG SSI), Diretor Nacional da Polícia de Segurança Pública (DN PSP), Comandante-Geral da Guarda Nacional Republicana (CG GNR), Diretor Nacional da Polícia Judiciária (DN PJ), Diretor Nacional dos Serviços de Estrangeiros e Fronteiras (DN SEF), dirigentes máximos dos OPC de competência específica e o Diretor-Geral dos Serviços Prisionais).

O conselho coordenador tem como competências principais dar orientações genéricas para assegurar a articulação entre os OPC, garantir a adequada coadjuvação das autoridades judiciárias por parte dos órgãos de polícia criminal, bem como definir metodologias de trabalho e ações de gestão

informações entre as autoridades nacionais e as agências referidas, consideramos ter sido um retrocesso a decisão governamental, através da nova Lei orgânica da PJ de 2019, manter sob a alçada da Unidade de Cooperação Internacional, da Polícia Judiciária, os referidos gabinetes, mesmo após Portugal ter sido chamado à atenção pelas autoridades europeias da necessidade de os países-parte possuírem um "single point of contact", responsável pela coordenação da cooperação policial internacional, garantindo uma interlocução qualificada entre as polícias nacionais e os serviços europeus de polícia.

que favoreçam uma melhor coordenação e mais eficaz ação dos OPC nos diversos níveis hierárquicos (artigo 14.º, n.º 1 al. a) a f)).

Por seu turno, para além das competências previstas para o SG SSI, de coordenação, direção, controlo e comando operacional, elencadas no artigo 15.º e 16.º da LSI, no artigo 15.º da LOIC, sob a égide "sistema de coordenação" vêm previstas ainda outras competências, tais como o dever de, nomeadamente, nos termos das orientações genéricas emitidas pelo conselho coordenador, coordenar os OPC, sem prejuízo das competências do Ministério Público, entidade competente para dirigir o inquérito, conforme previsto no artigo 263.º, n.º 1 do CPP, velar pelo cumprimento da repartição de competências entre OPC de modo a evitar conflitos e garantir a partilha de meios e serviços de apoio de acordo com as necessidades de cada OPC.

Não obstante as competências previstas para o SG SSI de "coordenação dos órgãos de polícia criminal", cremos ser difícil tal vir a suceder, pelo menos no que concerne ao nível operacional, considerando o previsto no n.º 3 do já citado artigo 15.º da LOIC, que veda ao SG SSI a possibilidade de emitir diretivas, instruções ou ordens sobre processos determinados, sendo-lhe igualmente vedado a sua consulta, através do sistema integrado de informação criminal, pois não tem a qualidade processual necessária para o efeito (Autoridade Judiciária ou OPC).

Neste patamar, parece-nos muito difícil existir uma coordenação eficiente entre os OPC através do regime previsto, ficando na prática a coordenação operacional da investigação criminal entregue aos OPC diretamente protagonistas, sempre muito competitivos, como é do nosso conhecimento público, dificultando investigações criminais e pondo em causa os interesses e proteção imediata de vítimas, bem como o interesse público de realização da justiça, fins últimos do processo criminal.

A título exemplar e no que concerne ao tráfico de estupefacientes, no seguimento do previsto no Decreto-Lei n.º 81/95, de 22/04, existem, desde 1996, as unidades de coordenação e intervenção conjunta (UCIC), criadas nos termos do artigo 6.º, às quais compete disciplinar e praticar a partilha de informações oriundas de cada força e serviço integrante e a coordenação das ações que devam ser executadas em comum.

Não obstante, embora esteja previsto a existência de elementos das FSS nas UCIC respetivas, na realidade o mesmo não acontece, sendo a informação trocada à luz do protocolo em vigor gerida pela Polícia Judiciária (PJ), através da Unidade Nacional de Combate ao Tráfico de Estupefacientes (UNCTE), o que pode causar assimetrias no acesso da informação partilhada pelos OPC, e posteriores dificuldades na coordenação eventualmente a realizar em determinadas investigações criminais.

2.3 – Interoperabilidade entre as forças e serviços de segurança

Da dificuldade identificada de se efetuar uma coordenação eficiente entre os OPC, através do sistema de coordenação anteriormente referido, e dando seguimento ao previsto no artigo 11.º da LOIC, que prevê a existência de um "sistema integrado de informação criminal" que assegure a partilha de informações entre os OPC, de acordo com os princípios da necessidade e da competência, de modo a garantir a cooperação devida entre os OPC (artigo 10.º), foi publicada a Lei n.º 73/2009, de 12/08, com vista a estabelecer as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos OPC.

A implementação de uma plataforma dessa natureza visava, então, assegurar uma efetiva interoperabilidade dos OPC, para efeitos de realização de ações de prevenção e investigação criminal, por via dos seus sistemas de informação criminais, assegurando um elevado nível de segurança no intercâmbio de informações (artigo 2.º).

De facto, a plataforma de intercâmbio de informações criminais (PIIC) foi criada, contudo e tendo em consideração as restrições derivadas da própria Lei n.º 73/2009, nomeadamente o facto de os OPC manterem sistemas de informação criminais independentes e geridos por cada um deles, sem prejuízo dos níveis de acesso e de segurança que teriam de obrigatoriamente existir, a verdade é que na prática, por tais razões, a PIIC não se tem demonstrado como instrumento de facto que contribua, como devia, para o intercâmbio de informações necessárias à prevenção e repressão criminal, conquanto a gestão unitária da informação a integrar em tal plataforma pelos OPC obvia tal desiderato.

Ora, competindo ao SG SSI a implementação e coordenação geral do sistema, assegurar as funcionalidades de intercâmbio de informação, bem como a supervisão e segurança global da plataforma (artigo 5.º), competências que só efetivamente desenvolvidas serão oportunamente úteis, não podemos deixar de notar novamente as dificuldades de execução da dita supervisão pelo SG SSI, contando que lhe está vedado aceder aos elementos ou às informações do sistema integrado de informação criminal.

Em face das restrições que impendem sobre o SG SSI anteriormente referidas, consideramos como uma mais-valia a ponderar no futuro a criação de um ponto único de contato para a coordenação interna entre os OPC – à semelhança do criado para a cooperação policial internacional, como adiante veremos – mas com competências efetivas de supervisão e coordenação operacional, em especial quando perante conflitos de competência positivos entre OPC, cuja ação direta serviria para os dirimir eficazmente, o que neste caso consideraríamos haver uma verdadeira coordenação operacional entre OPC[55].

Quanto aos canais de cooperação policial internacionais supra delimitados são, a nível nacional, atualmente geridos pela PJ embora o Decreto Regulamentar n.º 7/2017, de 7/08 que estabeleceu a organização e o funcionamento do Ponto Único de Contato para a Cooperação Policial Internacional (PUC-CPI), entidade criada através do Decreto-Lei n.º 49/2017, de 24/05, tenha atribuído competências de coordenação da cooperação policial internacional ao PUC-CPI, a quem lhe compete assegurar o encaminhamento dos pedidos de informação nacionais e respetivo intercâmbio internacional de informações entre os serviços de polícia e as autoridades policiais estrangeiras.

Neste sentido legislativo, previu-se ainda que na dependência orgânica do PUC-CPI ficaria o Gabinete SIRENE, o Gabinete Europol e Interpol, contudo ainda não foi aprovado o Regulamento relativo aos procedimentos internos do

[55] Não olvidamos a existência do Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS), documento classificado, onde estão delimitadas e definidas as regras, bem como os procedimentos que deverão ser adotados, relativas à cooperação e coordenação da FSS, contudo se estivermos perante investigações criminais em curso conflituantes entre dois OPC, que se declarem competentes para o efeito, o PCCCOFSS não resolve o conflito em causa (investigações criminais não se compatibilizam com resoluções documentais prévias e antecipatórias de conflitos…).

PUC-CPI, conforme previa o n.º 6, do artigo 2.º do Decreto Regulamentar supra citado[56], que iria fixar os procedimentos internos do PUC-CPI.

Não obstante, por força do previsto no artigo 5.º, n.º 2, al. a), do Decreto-Lei n.º 137/2019, de 13 de setembro – Lei Orgânica da PJ (posterior ao Decreto-Lei n.º 49/2017, de 24 de maio, anteriormente citado e que criou o PUC-CPI), ainda compete à PJ assegurar o funcionamento da Unidade Nacional EUROPOL (UNE) e do Gabinete Nacional INTERPOL (GNI), o que não deixa de causar estranheza a "técnica" legislativa utilizada que veio permitir a manutenção e funcionamento dos gabinetes UNE e GNI na dependência da Unidade de Cooperação Internacional da PJ depois de ter sido criado um Órgão, precisamente, com competências para a coordenação da cooperação policial internacional e gestão desses gabinetes, que se devia constituir como "balcão único" de gestão destas matérias[57].

Acresce ao referido que o previsto no artigo 12.º, n.º 1 da LOIC, que prevê que o funcionamento da UNE e do GNI compete à PJ, ficaria prejudicado pelo Decreto-Lei n.º 49/2017 e pelo recente Decreto-Lei n.º 10/2020, não fosse a Lei Orgânica da PJ vir, afinal, "devolver" a competência à PJ de, através da Unidade de Cooperação Internacional, assegurar o funcionamento da UNE e do GNI (artigo 5.º, n.º 2, al. a) da Decreto-Lei n.º 137/2019).

Em suma, embora as razões subjacentes à criação do PUC-CPI[58], bem descritas no preâmbulo do Decreto-Lei n.º 49/2017, nomeadamente a necessidade de "reforço das sinergias e da cooperação a todos os níveis para uma resposta eficaz e coordenada a nível nacional, europeu e internacional" com garantia de "uma interlocução qualificada" para melhor resposta às

[56] Regulamento entretanto revogado pelo artigo 8.º do Decreto-Lei n.º 10/2020, de 11/03, que veio estabelecer a orgânica do Ponto Único de Contacto para a Cooperação Policial Internacional, sem dar solução ao problema identificado no texto.

[57] Embora seja de referir que veio a público a notícia de que a UNE e o GNI passariam para dependência direta do ponto único de contato para a cooperação policial internacional, na dependência do Secretário-Geral do Sistema de Segurança Interna, a verdade é que, até esta data, por força da resistência da Polícia judiciária, tal não ocorreu, existindo novos desenvolvimentos indicando que, ainda que a UNE e GNI passem para a estrutura "física" do SSI, será a PJ a manter a gestão exclusiva dos respetivos gabinetes. Obtido de https://www.dn.pt/sociedade/pj-cede-europol-e-interpol-a-seguranca-interna-mas-tem-pacto-para-manter-a-gestao-exclusiva-15110537.html.

[58] Salientadas, igualmente, no Relatório Anual de Segurança Interna de 2019, pp. 192-194. Embora neste RASI se assuma que em resultado da avaliação da aplicação do acervo Schengen a Portugal, relativo à cooperação policial, se tenham detetado deficiências e lacunas a corrigir, tendo sido enviado documento à "COM" com o plano de ação e respetiva calendarização das correções elencadas, este Relatório não as identifica.

exigências da cooperação entre as autoridades competentes dos Estados-Membros da EU, necessidades que já constavam nomeadamente na Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020 [59], projetando-se o PUC-CPI como um "balcão único", em conformidade com as orientações para a criação de um ponto único de contato para o intercâmbio internacional de informação entre serviços de polícia"[60], que deveria reunir sob a mesma estrutura de gestão e no mesmo espaço físico os diferentes gabinetes nacionais ou pontos de contato relevantes (Gabinete Nacional Sirene, o Gabinete Nacional Interpol e a Unidade Nacional da Europol)[61], mal grado Portugal, nas diversas avaliações Schengen, ter sido já chamado à atenção por ainda não ter dado cumprimento à criação de um "Single Point of Contact", causando alguma estupefação o fato de se ter vindo a sobrepor a decisão de manter sob a alçada da PJ, na sua Unidade de Cooperação Internacional, a UNE e o GNI, através da sua Lei orgânica, como referimos anteriormente.

2.4 – Conclusão capitular

A cooperação policial internacional é fundamental na prevenção e combate ao crime organizado transnacional, permitindo um rápido intercâmbio e partilha de informações criminais relevantes, que possibilitam às Autoridades policiais agir com maior rapidez e eficiência na deteção e combate a diversas ameaças e riscos que coloquem em causa a segurança interna e a ação preventiva das autoridades policiais.

Considerámos relevante destacar o papel da Europol, da Interpol e dos Gabinetes Nacionais Sirene, no âmbito da prevenção e combate à criminalidade organizada, que fornecem informações e apoio na recolha, análise, tratamento e partilha de informação criminal, entre os Estados-Membros da UE, relativas a organizações criminosas.

[59] Documento 9798/15, de 10 de junho de 2015, JAI 442 COSI 67, disponível em https://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/pt/pdf.
[60] Doc. 10492/14, de 13 de junho de 2014, DAPIX 75 ENFOPOL 157, disponível em https://db.eurocrim.org/db/en/doc/2214.pdf, que define as linhas condutoras relativas à figura do Single Point of Contact (SPOC).
[61] Referimo-nos apenas a estes três, que são os pontos de contato objeto do nosso estudo.

Neste âmbito, cumpriu destacar, no que concerne ao crime organizado cometido através do ciberespaço, o Centro de Inovação da UE para a segurança interna, composta por representantes das agências europeias e instituições da UE, que objetivam garantir informação atualizada aos EM, fornecer soluções tecnológicas aos mesmos, que aumentem sinergias comuns, de modo a desenvolver ferramentas (software e inteligência artificial) para melhorar a prevenção e repressão do crime organizado cometido através da internet, designadamente através da darknet.

A utilização dos diversos canais de cooperação policial internacional obedecem a coordenação interna prévia dentro do quadro regulamentar de cada país membro, estando atualmente estabelecido que o funcionamento das unidades responsáveis pela centralização e tratamento de informação proveniente da UNE e do GNI são asseguradas pela PJ, pelo que, para outros OPC beneficiarem de informação útil e oportuna daquelas agências internacionais, é necessário que haja, previamente, uma coordenação entre os diversos OPC e a PJ, que funcione de forma fluída, de modo a contribuir para a luta contra a criminalidade organizada transnacional existente, cujo interesse é nacional.

Neste patamar, consideramos mister, para garantir a necessária e potenciada interoperabilidade entre as forças e serviços de segurança, com competência no combate ao crime organizado transnacional, a criação no futuro de um ponto único de contato para a coordenação interna entre os OPC, com competências efetivas de supervisão e coordenação operacional, cuja ação direta serviria para dirimir conflitos entre investigações, que ocorrem recorrentemente, garantindo uma verdadeira coordenação operacional entre OPC, que a implementação da PIIC (2009) revelou não garantir.

Deste modo, garantindo-se, a montante, uma eficiente coordenação policial interna, consideramos fundamental que se avance, finalmente, com um "single point of contact", sediado no SSI, que seja efetivamente responsável pela coordenação da cooperação policial internacional, como garante de uma interlocução qualificada entre as polícias nacionais e as agências europeias e internacionais de polícia, sem necessidade de mediação da informação criminal por parte de um só OPC, que atualmente funciona como pivot, em nada

acrescentando às investigações criminais que decorrem, sob delegação das Autoridades judiciárias competentes, nos diversos OPC.

CAPÍTULO 3

PREVENÇÃO E INVESTIGAÇÃO DO CRIME DE TRÁFICO DE ESTUPEFACIENTES

3.1 – Atividade da Polícia. Da prevenção à repressão

Conforme expende a Lei n.º 53/2007, de 32/08 – Lei Orgânica da Polícia de Segurança Pública (PSP), a PSP é uma força de segurança, uniformizada e armada, com natureza de serviço público e dotada de autonomia administrativa, encontrando-se hierarquicamente organizada, estando o pessoal com funções policiais sujeito à hierarquia de comando e o pessoal sem funções policiais sujeito às regras gerais da hierarquia da função pública, cuja missão é a de assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, nos termos da Constituição e da Lei (artigo 1.º).

A Constituição da República Portuguesa, logo nos seus primeiros artigos, elenca de forma genérica no artigo 9.º quais as "Tarefas fundamentais do Estado", destacando-se na al. b), como um dos princípios fundamentais a prosseguir pelo Estado a garantia dos direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático, constituindo o artigo 27.º, n.º 1 da Lei fundamental como um dos corolários daquele princípio ao referir que "todos têm direito à liberdade e à segurança".

Nesse âmbito, prevê o artigo 272.º, n.º 1 da CRP que, para alcançar os desígnios fundamentais elencados anteriormente em ordem a garantir os direitos, liberdades e garantias dos cidadãos, cabe à Polícia defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos.

Deste último preceito mencionado, cabe remissão reflexa para a Lei de Segurança Interna (LSI) importando, desde logo, destacar o enunciado no artigo 1.º que refere "A segurança interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade (…)".

Dos preceitos referidos consegue-se retirar que é tarefa fundamental do Estado garantir a segurança e tranquilidade públicas, bem como proteger as pessoas e bens, tarefa essa desenvolvida, precisamente, através da adoção de políticas públicas de segurança que devem constar nas estratégias definidas pelas entidades governativas, objetivos que só podem ser alcançados com a adoção, em primeiro lugar, de estratégias e políticas públicas de segurança e, depois, com a concretização de planos de ação objetivos/operacionais, estes últimos a serem prosseguidos pelas forças e serviços de segurança com competência nas respetivas matérias de segurança.

As suas atividades são desenvolvidas de acordo com os objetivos das políticas públicas de segurança, objetivos esses definidos a nível governamental, mas respeitando a sua missão e enquadramento orgânico, legalmente definido conforme suprarreferido, sendo que em casos de situação de exceção, as suas atribuições são as decorrentes da legislação sobre a defesa nacional, estado de sítio e estado de emergência[62].

A PSP depende do membro do Governo responsável pela Administração Interna, a sua organização é única para todo o território nacional (prosseguindo atribuições em todo o território nacional, excluindo as áreas legalmente atribuídas a outras forças e serviços de segurança) e está organizada hierarquicamente em todos os níveis da sua estrutura com respeito pela diferenciação entre funções policiais e funções gerais de gestão e administração públicas, obedecendo quanto às primeiras à hierarquia de comando e quanto às segundas às regras gerais de hierarquia da função pública[63].

O grande enfoque da atividade da PSP é na prevenção de crimes e na ordem pública[64]:

- Prevenir a Criminalidade e a prática dos demais atos contrários à Lei e aos Regulamentos;
- Prevenir a criminalidade organizada e o terrorismo, em coordenação com as demais forças e serviços de segurança;
- Garantir a segurança das Pessoas e dos seus bens;

[62] https://www.psp.pt/Pages/sobre-nos/quem-somos/o-que-e-a-psp.aspx.
[63] *Idem.*
[64] *Idem.*

- Garantir a segurança rodoviária, nomeadamente através do ordenamento, fiscalização e regularização do trânsito;
- Garantir a segurança nos espetáculos desportivos e equiparados.

Como se depreende do referido anteriormente, a PSP é devedora de uma panóplia de atribuições e competências, cujo credor principal é o Cidadão, podendo hoje afirmar-se plenamente como uma Polícia integral (Elias, 2018).

No mesmo sentido, a PSP tem desenvolvido a sua atividade com bastante fulgor, principalmente nos últimos anos, na área da investigação criminal, prosseguindo as atribuições que lhe são acometidas pelo Código de Processo Penal e pela Lei de Organização da Investigação Criminal.

Seguindo Elias (2018), a investigação criminal pode ser definida como o conjunto de ações tendentes a descobrir, recolher, examinar, interpretar, conservar e formalizar no inquérito, as provas de factos concretos penalmente relevantes, podendo se afirmar que ao investigar determinada tipologia criminal, no seio do Sistema de Investigação Criminal, a PSP também promove a sua prevenção, bem como de outras tipologias conexas, adotando medidas especiais de prevenção e acompanhando de forma sistemática e permanente os locais de ocorrências criminosas frequentes, com recolha sistemática de informações relevantes para investigações presentes, futuras ou conexionadas.

Para efeitos de prevenção, investigação criminal, exercício da ação penal e execução de penas e medidas de segurança, foi aprovada a Lei-quadro de política criminal, através da Lei n.º 17/2006, de 23 de maio, ficando estabelecido que, bienalmente, o Governo, através da condução da política geral do país, apresentaria à Assembleia da República propostas de lei sobre os objetivos, prioridades e orientações de política criminal (artigo 7.º), com o objetivo de "prevenir e reprimir a criminalidade e reparar os danos individuais e sociais dela resultante, tomando em consideração as necessidades concretas de defesa dos bens jurídicos" (artigo 4.º).

Neste sentido, através da Lei n.º 55/2020, de 27 de agosto, foi aprovada a Lei de Política Criminal, com a respetiva definição de objetivos, prioridades e orientações para o biénio 2020-2022, constando como objetivos específicos de política criminal "prevenir, reprimir e reduzir a criminalidade violenta, grave e altamente organizada (…) [e] a cibercriminalidade" (al. a), artigo 3.º), incluindo como crimes de prevenção prioritária (al. b) e d), artigo 4.º) e, no que concerne

à cibercriminalidade, os crimes cometidos por meio de um sistema informático ou de comunicações, que são, igualmente, considerados crimes de investigação criminal prioritária.

No que toca ao crime de tráfico de estupefacientes e ou de substâncias psicotrópicas, embora constem do elenco de crimes incluídos como crimes de prevenção prioritária (al. b), artigo 4.º), e não sejam considerados, diretamente, crimes de investigação prioritária, cremos ser possível, através da inclusão dos crimes de tráfico de estupefacientes noutras alíneas, tais como al. e) e al. f), como crime cometido através de sistema informático ou comunicação, ou crime praticado de forma organizada ou em grupo, respetivamente, que aquela tipologia criminal possa beneficiar do regime previsto para os crimes de investigação prioritária, ínsito no artigo 6.º da Lei de Política Criminal.

Colhendo este argumento, como crimes de investigação prioritária, usufruem, nomeadamente, de "atribuição de prioridade (…) [e] precedência na investigação criminal e na promoção processual sobre processos que não sejam considerados prioritários", pois a "seleção dos crimes de prevenção e investigação criminal prioritárias [assenta] na informação disponibilizada no [RASI] de 2019, numa leitura concertada com as análises da EUROPOL em matéria de tendências do crime transnacional nas suas distintas dimensões de materialidade e gravidade" (Lei n.º 55/2020) e, como temos vindo a demonstrar, a criminalidade organizada transnacional, nomeadamente a cibercriminalidade em geral, e o *cyber* tráfico de estupefacientes, em especial, tem vindo a prosperar.

3.2 – Regime jurídico do tráfico de estupefacientes

O Regime jurídico aplicável ao tráfico e consumo de estupefacientes e substâncias psicotrópicas encontra-se plasmado no Decreto-Lei n.º 15/93, de 22 de janeiro, diploma que nasce, conforme se refere no seu preambulo, baseado na Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas de 1988, da qual Portugal faz

parte integrante [65], tendo essencialmente como objetivos principais privar aqueles que se dedicam ao tráfico de estupefacientes do produto das suas atividades, adotar medidas adequadas ao controlo e fiscalização dos precursores, produtos químicos e solventes, substâncias utilizáveis no fabrico de estupefacientes e de psicotrópicos, colmatar "brechas" e potenciar os meios jurídicos de cooperação internacional em matéria penal, bem como organizar, no plano interno, as tabelas de substâncias consideradas ilícitas, remetidas sistemicamente para os anexos deste diploma.

A partir do capítulo II do mencionado diploma encontra-se desenvolvido as previsões e punições, relativas ao crime de tráfico, branqueamento e outras infrações, relevando o artigo 21.º - tráfico e outras atividades ilícitas, como o artigo base de punições do tráfico de substâncias estupefacientes, abarcando uma panóplia de situações[66], as quais preenchidas, originam à perseguição penal e investigação criminal de suspeitos, cujas penas previstas são aumentadas de um quarto nos seus limites mínimo e máximo se, entre outras situações previstas, "o agente participar em outras atividades criminosas organizadas de âmbito internacional" (al. f), artigo 24.º) o que, como vimos anteriormente, é comum ocorrer, considerando que as organizações criminosas transnacionais praticam, em regra, diversos ilícitos em conjunto com o crime de tráfico de estupefacientes, considerando-se "equiparadas a casos de terrorismo, criminalidade violenta ou altamente organizada as condutas que integrem os crimes previsto nos artigos 21.º a 24.º e 28.º do presente diploma" (n.º 1, artigo 51.º), beneficiando das disposições correspondentes, em conformidade com o artigo 1.º, n.º 2 do CP.

No que concerne à investigação criminal propriamente dita, o artigo 57.º, n.º 2 prevê as situações em que a investigação dos crimes de tráfico ilícito de estupefacientes se presume deferida à PSP (a à GNR), quando praticados nas respetivas áreas de jurisdição, quando lhes forem participados ou deles colham

[65] Convenção assinada e ratificada internamente através da Resolução da Assembleia da República n.º 29/91 e Decreto do Presidente da República n.º 45/91, publicados no Diário da República, de 6 de setembro de 1991.

[66] **Artigo 21.º Tráfico e outras atividades ilícitas.**

1 – *Quem, sem para tal se encontrar autorizado,* ***cultivar, produzir, fabricar, extrair, preparar, oferecer, puser à venda, vender, distribuir, comprar, ceder ou por qualquer título receber, proporcionar a outrem, transportar, importar, exportar, fizer transitar ou ilicitamente detiver****, fora dos casos previstos no artigo 40.º, plantas, substâncias ou preparações compreendidas nas tabelas I a III é punido com pena de prisão de 4 a 12 anos.*

notícia, quando, refere a al. a) do mesmo preceito, "ocorram situações de distribuição direta aos consumidores, a qualquer título, das plantas, das substâncias ou preparações nele referidas", o que, a nosso ver, não deixa de ocorrer sempre no crime de tráfico de estupefacientes, pois o objetivo último do traficante é fazer chegar a substância estupefaciente ao consumidor final, ainda que através de intermediários vários, independentemente da forma, meio ou "título" em que as substâncias estupefacientes são distribuídas, a final.

Neste sentido, consideramos que a investigação do crime de tráfico de estupefacientes e substâncias psicotrópicas se encontra, sempre, na área concorrencial de atuação, tanto da PJ, GNR ou PSP, presumindo-se o OPC competente para investigação o órgão a quem for participado ou tenha colhido notícia do respetivo crime, praticado na sua área de jurisdição[67].

Note-se que o sentido desta interpretação merece acolhimento no Decreto-Lei n.º 81/95, de 22 de abril que, logo no seu preâmbulo, afirma que "urge, assim, face à disseminação do fenómeno [tráfico e consumo de estupefacientes e substâncias psicotrópicas] empenhar no esforço direto de combate à oferta e ao consumo outros órgãos de polícia criminal [que não a polícia judiciária], a cuja preparação técnica se tem atendido", pelo que consideramos inexistir sustentação para afirmar que, mediante vicissitudes várias e normais nos circuitos de tráfico de estupefacientes, esta ou aquela Polícia é o OPC competente para investigar o crime de tráfico de estupefacientes, nomeadamente o tráfico proveniente de países estrangeiros[68].

Em termos de prevenção criminal do crime de tráfico de estupefacientes e substâncias psicotrópicas, de acordo com o DL n.º 81/95, cabe especialmente à PSP, na sua área de atuação, "a vigilância dos recintos predominantemente frequentados por grupos de risco" e a "a vigilância e o

[67] Ademais, constitui atribuição da PSP, especificamente, "prevenir e detetar situações de tráfico e consumo de estupefacientes ou outras substâncias proibidas, através da vigilância e do patrulhamento das zonas referenciadas como locais de tráfico ou consumo", cf. al. m), n.º 2, do artigo 3.º da Lei n.º 53/2007, de 31 de agosto (Lei que aprovou a orgânica da Polícia de Segurança Pública). Obtido de https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1079&tabela=leis.

[68] Neste sentido, e na mesma linha de raciocínio, a al. i) do n.º 3, do artigo 7.º da LOIC, prevê que é ainda da competência reservada da Polícia Judiciária a investigação" Relativos ao tráfico de estupefacientes e substâncias psicotrópicas, tipificados nos artigos 21.º, 22.º, 23.º, 27.º e 28.º do Decreto-Lei n.º 15/93, de 22 de janeiro, e dos demais previstos neste diploma **que lhe sejam participados ou de que colha notícia**" (negrito nosso). Consideramos, pois, ser esse o fator distintivo de atribuição de competências de investigação a OPC, e não outro.

patrulhamento das zonas usualmente referenciadas como locais de tráfico ou de consumo" (al. a) e al. b), respetivamente, do n.º 2 do artigo 2.º).

No que concerne à centralização de informação e coordenação operacional, é atribuída à PJ, através da Direção Central de Investigação do Tráfico de Estupefacientes, atualmente Unidade Nacional de Combate ao Tráfico Estupefacientes (UNCTE), a competência para tratamento de toda a informação respeitante às infrações tipificadas no DL n.º 15/93, de 22 de janeiro (n.º 1, do artigo 4.º), cabendo aos restantes OPC e serviços aduaneiros e de segurança transmitirem, no imediato, todas as informações que obtenham relativas à "preparação ou início da execução de quaisquer das infrações previstas no diploma mencionado no número anterior" (n.º 2, do artigo 4.º), o que o faz nos termos densificados no Protocolo das Unidades de Coordenação e Intervenção Conjunta (UCIC), firmado em outubro de 1996, entre os vários OPC e os serviços aduaneiros e de segurança com responsabilidade no combate ao tráfico de droga, com o objetivo de prevenir a intrusão ou contusão entre investigações e a garantir o intercâmbio fluído de informação disponível em cada força policial ou serviço aduaneiro e de segurança sem quebra da operatividade das investigações, a assegurar através das Unidades de Coordenação e Intervenção Conjunta (UCIC), sob a coordenação e direção estratégica e tática da PJ.

3.3 – Competências investigatórias da PSP

As competências de investigação criminal da PSP, inerentes à sua natureza de guardião da legalidade democrática, fundamentam-se, desde logo, na sua Lei Orgânica[69], prevendo a al. e), do n.º 2 do artigo 3.º, que constitui atribuição da PSP "desenvolver as ações de investigação criminal (…) que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas".

Por seu turno, a LOIC, já anteriormente mencionada, que define a investigação criminal como "conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as

[69] Lei n.º 53/2007, de 31 de agosto, atualizada pela Lei n.º 73/2021, de 12 de dezembro.

provas, no âmbito do processo" (artigo 1.º), atribui competência genérica à PSP, a par da PJ e GNR, de investigação criminal, competindo-lhe "coadjuvar as autoridades judiciárias na investigação" e "desenvolver as ações de prevenção e investigação da sua competência ou que lhes sejam cometidas pelas autoridades judiciárias competentes" (artigo 3.º, n.º 1 e 4, al. a) e b)).

Neste domínio, a PSP é competente para a investigação dos crimes cuja competência não esteja reservada a outros OPC, nomeadamente à PJ, nos termos do previsto no artigo 7.º, ou de crimes cuja competência lhe tenha sido delegada genericamente, nos termos do artigo 270.º, n.º 4 do CPP, conforme previsto na circular n.º 6/2002, de 11 de março, da Procuradora-Geral da República.

No que concerne, em específico, ao tráfico de substâncias estupefacientes, refere a al. i), do n.º 3 do artigo 7.º, que é da competência reservada da PJ a investigação de crimes relativos ao tráfico de estupefacientes e de substâncias psicotrópicas (…) que lhe sejam participados ou de que colha notícia. Como referimos anteriormente, consideramos que a referência a "de que colha notícia" se refere a coleta ativa de notícia de crime de tráfico de estupefacientes e não por força da informação remetida pelos outros OPC, nos termos da centralização prevista no artigo 4.º do DL n.º 81/95.

Quanto a crimes informáticos e praticados com recurso a tecnologia informática (al. l), n.º 3, do artigo 7.º da LOIC), que também fazem parte do elenco de crimes inseridos na competência reservada de investigação da PJ, considera-se importante referir que, atualmente, os grupos organizados de criminosos, tal como definimos previamente, fazem uso recorrente das novas tecnologias de informação e de ferramentas tecnológicas de comunicações, indispensáveis ao desenvolvimento da sua atividade ilícita.

Neste patamar, importa questionar se determinados crimes, que se inserem na competência concorrencial entre OPC de competência genérica – PSP, GNR e PJ, por serem praticados com recurso a tecnologia informática podem, apenas, ser investigados pela PJ, como por exemplo crimes da competência de investigação da PSP, nomeadamente o crime de tráfico de substâncias estupefacientes, em que os suspeitos socorrem-se, recorrentemente, à internet para se contactarem entre si, efetuarem transações ou combinarem *modus operandi*.

Quanto a esta questão existe um entendimento da Procuradoria-Geral Distrital de Lisboa, que tem vencido entre a doutrina Policial e Ministério Público, que refere que:

> (…) existe a possibilidade de se fazer a distinção entre "crimes informáticos" e "crimes cometidos com meios informáticos", associando aos primeiros a vocação da Polícia Judiciária, enquanto corpo superior investigação criminal, para a investigação do crime de maior complexidade, sendo esses crimes os que envolvem, como atributo indissociavelmente no seu cometimento, o uso ou o ataque à tecnologia informática, como é o caso dos tipos previstos na Lei n.º 109/2009 ou a exploração de conteúdos pornográficos de menores na internet" e que "Outros ilícitos, de menor densidade, que podem usar meios informáticos no seu cometimento, não se confundirão com aqueles em virtude de os meios informáticos serem uma mera plataforma comunicacional não essencial como atributo da conduta criminosa, como serão, por exemplo, os casos das injúrias, das ameaças ou de condutas integrativas de maus tratos, quando cometidos por mensagem de correio eletrónico, ou ainda, difamações em blogues ou em fórum na internet,
>
> Estes ilícitos admitirão uma investigação realizada nos serviços do MP ou delegada em OPC de competência genérica, investigação que seja, ademais, compatível, no caso de crime de natureza particular, com o curto prazo de prescrição[70].

Colhendo o aludido entendimento, em face do anteriormente referido no capítulo 1, acerca das novas tendências e infiltrações do cibercrime na criminalidade organizada, sobreleva a urgência de a PSP, enquanto OPC com competências genéricas de investigação, e enquanto polícia integral, se

[70] Informação n.º 20/2010, do DIAP de Lisboa, de 26/04/2010 – Informação da PGDL: crimes cometidos pro meios informáticos. Ação de formação de 12/02/2010 (sublinhado nosso).

adaptar rapidamente às novas tecnologias, para fazer frente a toda uma panóplia de criminalidade, que por força das suas competências terá de investigar, relevando a necessidade de garantir uma estrutura orgânica central e de se apetrechar com tecnologias de suporte que garanta, no domínio das suas atribuições, a prevenção e combate de fenómenos criminais com utilização de meios informáticos, ferramentas tecnológicas e meios de comunicação *online*.

Nesse patamar, a Portaria n.º 383/2008, que veio estabelecer a estrutura nuclear da Direção Nacional da Polícia de Segurança Pública e as competências das respetivas unidades orgânicas, no âmbito da investigação criminal, atribuiu, no artigo 6.º, diversas competências ao Departamento de Investigação Criminal, sendo de destacar as competências de coordenar as vertentes processual e operacional da atividade da PSP (al. a)) e de apoiar tecnicamente, propondo e difundindo instruções, em especial relativamente a crimes de maior gravidade, complexidade ou dispersão territorial, que justifiquem a gestão concentrada da investigação (al. b), vindo a se criar através do Despacho n.º 6158/2017, de 13 de julho [71], o Núcleo de cibercriminalidade, incluindo-o na Divisão de Investigação Criminal e Cooperação Internacional, do Departamento de Investigação Criminal.

De facto, e como se refere no preâmbulo do Despacho mencionado, em face da "evolução tecnológica na área de comunicações e sistemas de informação", procurando-se "uma adequação mais ajustada a uma maior eficiência de processos na execução das respetivas atribuições", impunha-se alterações ao modelo organizativo de alguns Departamentos da DN PSP, designadamente do Departamento de Investigação Criminal.

Neste âmbito, nos termos da al. i), do n.º 1 do artigo 12.º, passou, também, a competir à Divisão de Investigação Criminal e Cooperação Internacional do DIC, através do Núcleo de cibercriminalidade, "apoiar a prevenção, a deteção e a investigação de crimes relacionados com a utilização de meios informáticos no âmbito das competências da PSP", apoiando investigações que corram termos nos diversos Comandos de Polícia,

[71] Que alterou o Despacho n.º 19935/2008, de 17 de julho, alterado e republicado pelo Despacho n.º 11714/2010, de 23 de junho, as unidades orgânicas flexíveis da Direção Nacional da PSP, bem como as correspondentes competências.

nomeadamente na extração e análise de cabeçalho técnicos de emails de *phishing*[72], e na recolha de dados/prova digital em apoio a inquéritos que decorram.

Trata-se aqui, quiçá, de o embrião para a PSP se assumir como polícia distinta no âmbito da prevenção de cibercrimes, através do patrulhamento sistemático do espaço cibernético (cibersegurança), principalmente através de fontes abertas, e, igualmente, na investigação de crimes praticados no ciberespaço (cibercriminalidade), nomeadamente, tráfico de substâncias estupefacientes através da internet.

Neste âmbito, cremos, que o Núcleo de cibercriminalidade terá de se expandir para outra dimensão macro, operando ao nível de uma Divisão de Coordenação de Cibercriminalidade, com núcleos especializados de cibersegurança, por um lado, e de investigação de cibercriminalidade, por exemplo, nas áreas do tráfico de estupefacientes, da violência no desporto, da venda de artigos pirotécnicos para utilização em manifestações de protesto ou nos recintos desportivos, por outro, à semelhança de outros OPC, como a PJ[73], em face da importância que configura a luta contra a cibercriminalidade, conforme referem os relatórios nacionais e internacionais anteriormente escalpelizados.

3.4 – Conclusão capitular

A Polícia de Segurança Pública, como polícia integral, abarca uma panóplia de atribuições, desde a prevenção de crimes à investigação criminal, como garante da legalidade democrática, a segurança interna e os direitos dos cidadãos, nos termos da Lei e da CRP, de forma a garantir os direitos, liberdades e garantias dos cidadãos (artigo 272.º CRP).

No seio do sistema de investigação criminal, a PSP, tem desenvolvido a sua atividade, sustentada no quadro previsto de repartição de competências ínsito na LOIC, promovendo a prevenção e investigação de crimes,

[72] Técnica de engenharia social usada para enganar utilizadores da internet, com o objetivo de obter informações confidenciais, como nome e detalhes de cartão de débito/crédito, cujo remetente parece de uma fonte confiável (Wikipédia, 2022).

[73] Nos termos do artigo 33.º do Decreto-Lei n.º 137/2019, de 13 de setembro, a PJ tem constituída uma Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, a quem compete dar resposta preventiva e repressiva ao fenómeno do cibercrime (n.º1).

desenvolvendo diversas ações e adotando medidas especiais de prevenção e acompanhamento, sistemático e permanente, de locais de frequência criminal, com recolha de informações para as investigações em decurso, bem como para futuras investigações.

Em termos de política criminal, para o presente biénio (2020-2022), o tráfico de estupefacientes ou de substâncias psicotrópicas foi elencado como um crime de prevenção prioritária, embora não conste no elenco dos crimes de investigação prioritária. Não obstante, cremos, em face das já referidas tendências do cibercrime, onde se inclui o tráfico de estupefacientes através da internet, ser possível integrar, reflexa ou indiretamente, o crime de tráfico de estupefacientes através da internet como crime de investigação prioritária, por força da previsão dessa prioridade investigatória para o crimes cometidos através de sistemas informáticos ou, mesmo, através dos crimes praticados de forma organizada ou em grupo, *modus operandi* inevitavelmente utilizado pelos traficantes, de modo a imprimir maior pujança *ope legis* à investigação do crime de tráfico de estupefacientes através da internet.

Articulando os argumentos discutidos neste capítulo, consideramos legítima a interpretação de que o crime de tráfico de estupefacientes e substâncias psicotrópicas, insere-se no âmbito da competência concorrencial dos diversos OPC de competência genérica, sendo o critério distintivo de atribuição de competência investigatória o *locus delicti* e a recolha ativa da notícia do crime, e não outros critérios como as ligações internacionais existentes no tráfico, que são inevitáveis considerando que Portugal não é um país produtor de estupefacientes, ou o facto de haver ou não distribuição direta ao consumidor, pois no tráfico essa distribuição existirá sempre, como objetivo final do processo produtivo de compra e venda ilegal de produtos estupefacientes.

No que concerne ao tráfico de substância estupefacientes cometido através de tecnologias ou meios informáticos, sustentados na informação da PGDL n.º 20/2010, tendo competências investigatórias plenas nesta tipologia criminal, urgindo importante, em face das novas tendências e infiltrações do cibercrime no tráfico de estupefacientes, a PSP, enquanto OPC com competência genérica de investigação, apostar no desenvolvimento de uma estrutura alocada em exclusivo, no domínio das suas atribuições, que lhe

permita eficazmente prevenir e combater fenómenos criminais com utilização de meios e ferramentas tecnológicas, à semelhança de outros OPC, como a PJ, em face da importância que configura a luta contra a cibercriminalidade, relatada no relatórios nacionais e internacionais que decidimos trazer à discussão.

CAPÍTULO 4

TRÁFICO DE ESTUPEFACIENTES COMETIDO ATRAVÉS DA INTERNET

4.1 – Delimitação conceptual

Conforme referido anteriormente, em Portugal o regime jurídico relativo ao tráfico de estupefacientes encontra-se previsto no Decreto-Lei n.º 15/93, de 22 de janeiro[74], entretanto atualizado por diversas vezes (29.ª versão – Lei n.º 25/2021, de 11 de maio).

Pese as diversas alterações legislativas que o diploma originário tem vindo a sofrer ao longo destes quase 30 anos, verificamos que o regime, previsto e punido pelo artigo 21.º e seguintes, não prevê especificamente o tráfico de estupefacientes através da *internet*, designadamente através da utilização da *dark web*[75].

Ora, como é bom de se ver as legislações que preveem determinados regimes de impacto societário elevado, nomeadamente os regimes jurídicos criminais, devem acompanhar a evolução das sociedades, adaptando-se às novas realidades e organizações criminosas.

De facto, na sociedade em que vivemos hoje são patentes as várias transmutações e evoluções, científicas e tecnológicas, como resultado da globalização (Lourenço, 2015), que nos trouxeram diversas formas de criminalidade complexa, onde se inclui o tráfico de estupefacientes, que, tal como o desenvolvimento económico, cultural e social, usufruíram da inserção da *internet*, atualmente de banda larga, servindo-se dos seus benefícios.

Considerando o sobredito, torna-se cada vez mais importante que as Autoridades competentes disponham de mecanismos para detetar atividades de tráfico de estupefacientes por via *online*, exigindo-se um esforço permanente para acompanhar a atividade criminosa de tráfico de

[74] Legislação de combate à droga. Obtido de https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=181&tabela=leis.

[75] Embora, no Regime jurídico da prevenção e proteção contra a publicidade e comércio das novas substâncias psicoativas, esteja previsto, no artigo 4.º, n.º 2, que a proibição de "produzir, importar, exportar, publicitar, distribuir, vender (…)", se estende à MO através de sítios na Internet.

estupefacientes com utilização tanto de canais e plataformas inseridas na internet "aberta" (*surface web*) como de canais inseridos na internet profunda (*Deep web*), de modo a prevenir, reprimir e combater este tipo de criminalidade.

Existe algum desconhecimento, e até confusão, relativamente à utilização dos vários conceitos correlacionados com a internet como *deep web*, *darknet*, *dark web* e *surface web*[76].

Este último conceito abarca os conteúdos que usual e diariamente todos nós acedemos, de livre acesso, onde encontramos documentos, imagens e ficheiros de documentos que estão registados e identificados por endereços eletrónicos, bastando escrever o respetivo endereço, ou apenas termos descritores, para acedermos à informação ou ao sítio que desejamos, como por exemplo ao Youtube ou ao Facebook.

Por seu turno, a *deep web* corresponde à parte da *internet* que não está registada e que não pode ser acedida da forma usual a que estamos habituados, contendo uma imensidão de informação inacessível aos motores de busca tradicionais.

Somente uma pequena porção de informação está diretamente acessível ao utilizador comum da *internet* que, segundo especialistas, representa apenas 4 % de todo o conteúdo que a *web* tem para oferecer, estimando-se que a *deep web* tenha um tamanho de 500 vezes superior ao da *surface web*, sendo que para ali aceder se exija um *software*, refira-se gratuito, de pesquisa de informação denominado TOR (*the onion route*), que permite navegar naquelas profundezas sob o anonimato[77].

A *deep web* abrange todas as páginas da *web* que os mecanismos de pesquisa convencionais não conseguem encontrar, sendo utilizada para fins lícitos, contendo bancos de dados de utilizadores, páginas *webmail* e páginas de "*paywalls*", mas também para fins ilícitos diretamente através da *darknet* ou através da *dark web*, *websites* que apenas podem ser acedidos através da

[76] What is the Dark Web, What's on it & How to Access it. (2019, 25 de outubro). Obtido de https://www.techadvisor.com/article/727316/what-is-the-dark-web-whats-on-it-how-to-access-it.html.
[77] *Idem*.

darknet[78], onde encontramos mercados ilícitos, sobrelevando o tráfico de estupefacientes, como veremos adiante.

Percebemos, então, que a utilização da *internet* profunda (*deep web*) existe tanto para fins lícitos, como para fins ilícitos, sendo que neste último os criminosos utilizam a *dark web* e a *dark net*, sob a capa do anonimato, para desenvolver as suas atividades ilícitas, por regra através de plataformas criadas para o efeito que servem de intermediários do acesso a produtos ilegais, onde figura o tráfico de estupefacientes, sobrelevando dificuldades acrescidas na identificação dos utilizadores, tendo em consideração que, nestes casos, estamos perante comunicações encriptadas anónimas, como vimos anteriormente.

Mas, importa referir também que, como é consabido, a denominada *internet* de superfície (*surface web*) também pode ser utilizada para fins ilícitos, sendo importante que as autoridades estejam atentas e ajam com rapidez no sentido de identificar as atividades delituosas e os criminosos que as desenvolvem e encetar as competentes investigações.

Nestes últimos casos, consideramos de relevar algumas particularidades do regime em vigor no nosso ordenamento jurídico de compra e venda de produtos e serviços através da *internet*, pois através de *sites* legítimos muitas das vezes são efetuados negócios ilegais e praticado tráfico de substâncias estupefacientes, sem que se verifique a sua deteção precoce e oportuna.

4.2 – O comércio eletrónico lícito (*e-commerce*)

O regime de negócios lícitos de compra e venda através da *internet*, denominado comércio eletrónico, encontra-se plasmado no Decreto-Lei n.º 7/2004, de 7 de janeiro, atualizado na sua 4.ª versão pela Lei n.º 40/2020, de 18 de agosto, e surge no ordenamento jurídico nacional por força da transposição da Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços de sociedade de informação, em especial do comércio eletrónico, no mercado interno.

[78] *Idem ibidem*.

Como referido no preâmbulo do citado Decreto-Lei o legislador ordinário optou, à imagem da diretiva que lhe serviu de base, por afastar soluções mais amplas e ambiciosas para a regulação do setor em causa, permitindo a aplicação subsidiária do Decreto-Lei n.º 143/2001, de 26 de abril, relativo aos contratos à distância, regime hoje previsto no Decreto-Lei n.º 24/2014, de 14 de fevereiro, que revogou aquele.

O regime de exercício da prestação de serviços através da "sociedade da informação" entende-se como um serviço prestado à distância por via eletrónica, no âmbito de uma atividade económica, na sequência de pedido individual do destinatário, prevendo-se um regime genérico de irresponsabilidade dos prestadores intermediários de serviços relativamente à eventual ilicitude das mensagens que disponibilizam, inexistindo portanto um dever geral de vigilância do prestador intermediário de serviços sobre as informações que transmite ou armazena ou, ainda, a que faculta o acesso, independentemente do tipo de contrato, sejam ou não qualificáveis como comerciais (artigo 11.º).

Não obstante, incumbe aos prestadores intermediários, como dever comum, informar de imediato as entidades competentes quando tiverem conhecimento de atividades ilícitas que se desenvolvam por via dos serviços que prestam (artigo 13.º), devendo informar de imediato o Ministério Público aquando detetem conteúdos disponibilizados por meio dos serviços que prestam, sempre que a disponibilização desses conteúdos, ou o acesso aos mesmos, possa constituir crime (artigo 19.º-A), sendo obrigados a assegurar, num prazo de 48 horas, o bloqueio dos sítios identificados (artigo 19.º-B).

Em termos de normas sancionatórias associadas à violação de tais deveres, prevê-se responsabilidade contraordenacional (artigo 37.º) e civil para os prestadores de serviços sempre que, perante as circunstâncias que conhecem, tenham ou devam ter consciência do caráter ilícito da informação (artigo 16.º), ou para os que, por meio de instrumentos de busca, hiperconexões ou processos análogos permitam o acesso a conteúdos ilícitos (artigo 17.º), bem como a possibilidade de aplicação de sanções acessórias de perda a favor do Estado dos bens usados para a prática das infrações, interdição do exercício da atividade pelo período máximo de seis anos e, tratando-se de pessoas singulares, a inibição do exercício de cargos sociais em

empresas prestadoras de serviços da sociedade de informação durante o mesmo período (artigo 38.º).

De referir que a entidade de supervisão central, com atribuições em todos os domínios regulados pelo diploma que vimos dissertando, é a Autoridade Nacional de Comunicações (ICP-ANACOM), nos termos do artigo 35.º que, como é bom de se ver, é um órgão administrativo sem especificações especiais, estando-lhe vedado desenvolver competências ou atribuições de órgão de polícia criminal (OPC), nomeadamente colher notícias dos crimes e impedir quanto possível as suas consequências, descobrir os seus agentes e levar a cabo os atos necessários e urgentes destinados a assegurar os meios de prova, conforme previsto no artigo 55.º do Código de Processo Penal (CPP).

Daqui se verificam as dificuldades existentes em prevenir atividades ilícitas conduzidas através da *internet* aberta ou de superfície (*surface web*), pois a entidade com competências de supervisão não possui atribuições que lhe permitam efetuar um verdadeiro patrulhamento cibernético, prevenindo crimes, que amiúde vão ocorrendo mesmo através de plataformas legítimas, servindo apenas de zelador das atividades dos prestadores de serviços intermédios.

No mesmo sentido, estes últimos, não obstante lhes incumbir, como dever comum, informar de imediato as entidades competentes quando tiverem conhecimento de atividades ilícitas que se desenvolvam por via dos serviços que prestem, sendo obrigados a assegurar, num prazo de 48 horas, o bloqueio dos sítios identificados, a verdade é que não existe um regime sancionatório forte, de tipo penal, podendo lhes apenas ser assacadas responsabilidades ao nível cível e ao nível do mero ordenamento social, com aplicação de eventuais sanções acessórias, tratando-se, na nossa perspetiva, de um regime dissuasório fraco perante os valores e bens jurídico que usualmente estão em causa (saúde pública, vida, integridade física, sociedade em geral) e que constam, sistematicamente, na legislação penal em vigor.

4.3 – Tráfico de estupefacientes através da internet (*cyber trafficking*)

A compra *online* de produtos estupefacientes tornou-se hoje uma realidade recorrente, seja derivada da situação pandémica em que vivemos recentemente, cujas "medidas implementadas introduziram perturbações muito significativas nos circuitos e nas dinâmicas do tráfico ilícito de estupefacientes" (Rasi, 2021, p. 60), seja por força natural do desenvolvimento das novas tecnologias, conforme frisamos anteriormente.

De facto, os grupos organizados de criminosos que se dedicam a esta tipologia criminal, de tráfico de substâncias estupefacientes e produtos psicotrópicos, têm vindo a adaptar-se a novas realidades, utilizando "mercados *online*, plataformas digitais, redes sociais e serviços de entrega rápida" (Idem).

A exploração de mercados ilícitos *online*, através da *dark web*, pelos grupos organizados de traficantes, que requer a utilização prévia de um browser especial (ex. Tor) para aceder, que no fundo se trata de uma plataforma que permite comunicações privadas e de difícil rastreamento, tem sido uma constante, o que, pelo carácter confidencial e encriptado das comunicações, dificultam a ação das autoridades policiais (Ramalho, 2013) na prevenção e combate do tráfico de estupefacientes *online*.

Por esse motivo referido, de difícil acesso pelas autoridades policiais, bem como pela sua "comodidade e confidencialidade", os consumidores de substâncias estupefacientes ilícitas, têm optado pela aquisição de substâncias ilícitas através da internet, protegendo a sua identidade, diminuindo assim o risco de ser identificado pelas autoridades policiais (Ferreira, 2018).

Como nos ensina João Ferreira, o processo de transação de substâncias ilícitas inicia-se com a inscrição num website, registado na *dark web*, pelo vendedor, que anuncia os seus produtos, preços, tempo de demora de entrega, entre outras informações, havendo websites mais evoluídos que contêm, igualmente, menções avaliativas dos seus compradores, garantindo maior fiabilidade ao vendedor e, por seu turno, maior confiança na compra por parte do consumidor (Ferreira, 2018).

Acedendo ao "menu", os compradores registados, efetuam as suas compras, sob a capa do anonimato e da confidencialidade no respetivo website

que, por mediar a transação, recebe uma percentagem do valor pago, usualmente pago através de criptomoedas, aquando da remessa da substância ao cliente final (Ferreira, 2018).

Depois, confortavelmente, o cliente final rececionará num posto de entrega de encomendas, ou mesmo na sua residência, o produto anteriormente encomendado através da internet. Como exemplo paradigmático, deixamos nota de um grande intermediário de venda de drogas, que funcionou alguns anos com sucesso, conhecido como "Silk Road"[79], mercado que operou através da *dark web*, que acabou por ser desmantelado pelas autoridades policiais. Através de novos empreendedores criminais, a verdade é que continuam a ser criados e a operar outros sites, inseridos na *dark web*, com o mesmo *core business* que o "Silk Road", que à medida em que são detetados pelas autoridades competentes são encerrados, mas, inevitavelmente, disseminam-se novos websites com frequência idêntica.

Neste patamar, considerando a existência de *websites* de venda ilegal de produtos estupefacientes e substâncias psicotrópicas, onde os consumidores efetuam as suas encomendas, confortável e confidencialmente, cabe às autoridades competentes dos EM capacitarem as autoridades policiais, com estrutura e meios, para se garantir uma melhor prevenção, deteção, monitorização e investigação destes mercados *online* de tráfico de estupefacientes, nomeadamente através do "reforço da capacidade para a investigação criminal designadamente no quadro de obtenção de prova digital" (Rasi, 2021, p. 165).

Nessa sequência, consideramos que importará, igualmente, dedicarmos especial atenção ao circuito que as substâncias efetuam até entrega final. As substâncias ilícitas, compradas através da internet, são depois entregues aos consumidores finais através de serviços de entrega rápida, conforme referimos anteriormente.

Importa, pois, garantir a monitorização permanente do tráfico de estupefacientes *online*, de modo a se conseguir perceber como é que as

[79] Este website de venda ilegal de substâncias "possuía 6 categorias de drogas, medicamentos sujeitos a receita médica (ou "prescriptions", 3953 anúncios ativos), cannabis (2661 anúncios ativos), psicadélicos (1539 anúncios ativos), estimulantes (1274 anúncios ativos), ecstasy (1059 anúncios ativos) e opióides (262 anúncios ativos)". (Decary-Hetu, Aldridge, 2014, cit. in., Ferreria, 2018, p. 34).

substâncias são expedidas, e depois, como são entregues, no fundo como chegam ao consumidor final. Chegando através de serviços de entrega porta-a-porta ou mesmo através de serviços de correios postais, consideramos importante que as autoridades policiais apostem na deteção de locais onde os produtos estupefacientes são armazenados, ainda antes do início da remessa dos produtos aos clientes finais, o que para tal existe a necessidade de investimento em diversas valências tecnológicas que permitam o desenvolver desse trabalho, bem como reputamos importante incrementar protocolos entre as Polícias e os serviços de entrega postais e de encomendas, de modo a, através destas entidades, se sinalizar mais rapidamente este tipo de *modus operandi*.

4.4 – Conclusão capitular

O tráfico de estupefacientes e substâncias psicotrópicas através da internet ou com aproveitamento de novas tecnologias não se encontra, especificamente, previsto nos *modi operandi* elencados legalmente na legislação relativa ao tráfico de estupefacientes, embora como argumentamos anteriormente, consideremos que a realidade prevista no artigo 21.º do DL n.º 15/93 abrange o tráfico através da internet, por força da expressão “ou por qualquer título” (n.º 1).

Neste domínio, importou-nos dar a conhecer os vários conceitos relacionados com o comércio ilícito de produtos estupefacientes, pelo que, neste capítulo, delimitamos conceitos como *surface web*, *deep web* e *darknet*, concluindo que o tráfico de estupefacientes por via da internet ocorre tanto através da internet visível como da obscura, de forma a percecionarmos melhor o impacto do espaço cibernético nos mercados ilícitos de droga.

No que concerne ao regime de negócios lícitos de compra e venda através da internet (*e-commerce*), trouxemos a lume alguns aspetos legais do regime, concluindo que a ANACOM, entidade central com competência de supervisão nos negócios prestados através da sociedade de informação, ou seja, dos serviços prestados à distância por via eletrónica, não dispõe de competências de OPC, expondo as dificuldades existentes em prevenir

atividades ilícitas conduzidas através da internet visível ou aberta (*surface web*).

Concluímos, também, que tanto o crime de tráfico de estupefacientes através da internet visível como da obscura são de difícil investigação, sendo este ultimo de muito difícil investigação, considerando que os traficantes utilizam a darknet para mascarar a sua atividade criminal, recorrendo a plataformas criadas especificamente para o efeito, que servem de intermediários, como se de pontos de venda à consignação se tratassem, sendo que nestes casos estamos perante comunicações entre compradores-vendedores encriptadas e anónimas, o que dificulta, acrescidamente, a identificação dos utilizadores.

A compra de produtos estupefacientes *online* é, efetivamente, uma realidade que não podemos negligenciar, sendo certo que os grupos organizados de criminosos têm se adaptado, com sucesso, a esta realidade, cumprindo às autoridades policiais competentes empreender esforços no seu combate, capacitados que estejam com estrutura e meios necessários, com "reforço da capacidade para a investigação criminal designadamente no quadro de obtenção de prova digital" (RASI, 2021, p. 165), o que compreende empenhar meios tecnológicos que garantam a monitorização permanente do tráfico de estupefacientes *online*, desde a encomenda, passando pela expedição, até à entrega ao consumidor final.

CAPÍTULO 5

NECESSIDADE DE AJUSTAMENTO LEGISLATIVO PERANTE NOVAS REALIDADES

5.1 – Da aplicabilidade da Lei do cibercrime ao crime de tráfico de estupefacientes através da internet

A Lei do Cibercrime foi aprovada pela Lei n.º 109/2009, de 15 de setembro, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, adaptando, igualmente, o direito interno à Convenção sobre o Cibercrime do Conselho da Europa.

Trata-se de uma Lei que, no essencial, estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico (artigo 1.º).

Refere o artigo 11.º, n.º 1, al. b) que as disposições processuais previstas no capítulo relativo a "Disposições processuais" se aplicam a processos relativos a crimes cometidos por meio de um sistema informático.

A questão que de momento se revela de importante discussão é a de saber se se pode considerar o crime de tráfico de estupefacientes através da *internet* como um crime cometido "por meio de um sistema informático" de forma a podermos apurar, desde logo, se o regime da Lei do Cibercrime poderá ser utilizado na sua investigação.

Como vimos anteriormente a inserção da *internet*, atualmente de banda larga, serve os grupos organizados de criminosos, que têm utilizado os seus benefícios para desenvolver a sua atividade criminosa.

Quanto ao tráfico de estupefacientes esta realidade não é exceção, pelo contrário os traficantes rapidamente se adaptaram às novas tecnologias, fazendo uso das mesmas, sob o anonimato e a longas distâncias, com um computador e uma ligação camuflada através do motor de busca TOR, via *deep web*, desenvolvendo a sua atividade delituosa, pacífica e impunemente,

considerando as dificuldades acrescidas que as autoridades têm na deteção e investigação deste tipo de crime.

Assim considerando, e perante a existência de uma grande ligação entre o quotidiano e a informática, tal qual as mudanças provocadas pelo desenvolvimento tecnológico têm necessariamente repercussões no Direito Penal, pelo que, deste modo, admitindo-se o risco de o conceito de criminalidade informática compreender demasiados comportamentos, (Azevedo, 2016) entendemos que o crime de tráfico de estupefacientes cometido através da *internet* pode ser integrado na "criminalidade informática", para efeitos de investigação e recurso às disposições processuais alargadas previstas na Lei do cibercrime, considerando que a utilização da informática, nestes casos, aumenta "exponencialmente a perigosidade para bens jurídicos, dificult[a] a deteção do seu cometimento e do seu agente ou agrav[a] de modo muito significativo as suas consequências" (Macedo, 2009).

De todo o modo, em face das especificidades do cometimento do crime de tráfico de estupefacientes através da *internet*, conjugadas com a dificuldade de deteção e investigação criminal a desenvolver, consideramos que as disposições processuais da Lei do Cibercrime sempre teriam aplicabilidade por força da al. c), do n.º 1, do artigo 11.º, pois trata-se de uma tipologia criminal com caraterísticas especiais com incidências sobre meio informático, logo "em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico".

No mesmo sentido, tendo em consideração a abrangência da norma tipificadora do crime de tráfico e outras atividades ilícitas, previsto no artigo 21.º do Decreto-Lei n.º 15/93, também neste âmbito consideramos que o conteúdo de proteção da norma compreende atividades de tráfico efetuadas por qualquer meio, onde se poderá subsumir as condutas típicas desenvolvidas através de meios informáticos e tecnológicos, via *internet*, eventualmente merecedor de agravação nos termos do artigo 24.º, nomeadamente, entre outras, por força da al. b), f) ou g).

Aqui chegados, na esteira de Eduardo Correia, concluímos que o tráfico de droga através da *internet* enquadra-se nos "crimes informáticos" em sentido amplo, pois o tratamento de dados e de informação por aquela via é objeto ou instrumento do crime ou, pelo menos, o crime em causa está intimamente

ligado à utilização de sistemas ou plataformas alojadas na *internet* (Correia, 2000).

Em face das dificuldades, já anteriormente enunciadas, de investigação do crime de tráfico de estupefacientes com recurso à *internet* – anonimato e deteção difícil, a utilização das disposições processuais previstas na Lei do Cibercrime revelam-se de extrema importância, pois configuram instrumentos mais incisivos e sofisticados a fim de recolher e produzir prova num ambiente onde avulta uma dificuldade acrescida pela sua natureza e funcionamento (Valente, 2009).

Por força da conclusão anterior, isto é, de considerarmos que o crime de tráfico de estupefacientes através da internet é, por força da sua natureza e circunstâncias, também ele um crime informático, ainda que em sentido amplo, as disposições legais e processuais previstas na Lei do Cibercrime têm total aplicabilidade na investigação desta tipologia criminal.

Consideramos de relevar a possibilidade, nos termos do artigo 12.º, de preservação dos dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, quando no decurso da investigação for necessário à produção de prova, tendo em vista a descoberta da verdade, podendo essa preservação ser, ainda que sem ordem da autoridade judiciária competente, ordenada pelo órgão de polícia criminal mediante autorização da Autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo, nestes casos, ser informada a autoridade judiciária no mais curto espaço de tempo, nos termos do artigo 253.º do CPP.

Por via do artigo 15.º é possível ao órgão de polícia criminal, obter dados informáticos específicos e determinados quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, sendo que tal pesquisa não carece de prévia autorização da autoridade judiciária, sem prejuízo da obrigatoriedade de comunicação imediata à autoridade judiciária competente em ordem à sua validação, quando se tratar de terrorismo, criminalidade violenta ou altamente organizada, onde se inclui o crime de tráfico de estupefacientes, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa, ou quando quem tiver a disponibilidade ou controlo desses

dados voluntariamente o consentir, desde que esse consentimento prestado fique, por qualquer forma, documentado.

Estes meios de obtenção de prova revelam-se de extrema importância tendo em consideração que permitem preservar dados probatórios, no imediato, sob pena de que os mesmos se possam vir a perder, alterar ou deixar de estar disponíveis em linha, cujo acesso se fará no decurso do processo para efeitos de produção de prova e permitem determinar informações importantes como o tipo de serviço de comunicação utilizado, o período de serviço, a identidade, a morada postal ou geográfica, os dados respeitantes à faturação e ao pagamento, bem como qualquer outra informação sobre a localização do equipamento de comunicação que estejam disponíveis (artigo 14.º).

À luz da Lei do Cibercrime são admissíveis também ações encobertas, no fundo vigilâncias eletrónicas, previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso do inquérito podendo se recorrer a meios e dispositivos informáticos nessas ações sendo que, nestes casos, aplicam-se *mutatis mutandis* as regras previstas para as interceções de comunicações (artigo 19.º).

Por fim, de relevar ainda, da previsão no artigo 20.º de que no âmbito da cooperação internacional, as autoridades nacionais devem cooperar com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, do crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de outubro, potencialidade esta que se cumula à já prevista no artigo 58.º do Decreto-Lei n.º 15/93, relativa à cooperação internacional em matéria penal.

Se é certo que as medidas elencadas anteriormente e previstas na Lei do Cibercrime diminuem as garantias dos suspeitos visados pelas investigações, por outro lado tratam-se de medidas essenciais para o sucesso de investigações criminais em ambiente digitais, contando com a rapidez com que os dados fluem e, desse modo, sem a aplicação deste meios de obtenção de prova, perder-se-iam prejudicando sobremaneira as investigações (Azevedo, 2016).

De facto, "o mundo actual é altamente conectado, opera a um ritmo acelerado e em constante mudança" (Elias, 2018, p. 301), pois a internet tem vindo cada vez mais a ser utilizada pelos grupos organizados de criminosos transnacionais, pelo que incumbe às autoridades responsáveis pela segurança interna adotarem estratégias capazes de fazer face às ciberameaças presentes na sociedade contemporânea, impondo-se que os analistas conheçam e dominem os conceitos tecnológicos de forma a poderem propor soluções adequadas de resolução, "com vista à tomada de decisão informada e adequada" (Elias, 2018, p. 302).

5.2 – Das competências de investigação

Não obstante o sobredito, tais desígnios parecem ser obstaculizados pelo facto de imperar em Portugal uma repartição rígida de competências de investigação, que inclui no elenco de competências reservadas apenas a um órgão de polícia criminal, *in casu* Polícia Judiciária, a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, conforme artigo 7.º n.º 3, al. l) da Lei de Organização da Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto.

É de notar, neste particular, que em face da evolução tecnológica a que modernamente assistimos, temática desenvolvida nos capítulos anteriores, no que concerne a esta restrição parece-nos de tal modo anacrónica que pode hipotecar o combate eficaz e eficiente à cibercriminalidade que, igualmente como referimos anteriormente, projeta-se hoje, e prospetiva-se que no futuro também, seja a forma de criminalidade mais utilizada pelos grupos organizados de criminosos, em claro aproveitamento dos benefícios da *internet*, em especial da darknet, bem como de plataformas *online* sofisticadas para desenvolver a sua atividade criminosa de forma anónima e impune.

Neste patamar, consideramos crucial haver uma alteração legislativa[80] que permita a outros OPC desenvolver a sua actividade investigatória de crimes através da *internet*, considerando a vulgaridade com que esta forma é utilizada pelos criminosos, contando que atualmente a PSP e a GNR detém de

[80] Em termos genéricos, Luís Elias, quando discute as ciberameaças em face do desenvolvimento tecnológico atual, faz referência à "obsolescência dos regimes legais dos Estados", considerando que, *mutatis mutandis*, pensamos ter aqui aplicabilidade.

formação e conhecimentos técnicos de elevada especialidade, também na área informática, e que em face da notória, porque do conhecimento público, falta de meios humanos na PJ, poder-se-iam constituir como fortes aliados no combate a este flagelo.

Pensamos ser ainda de acrescentar que, mesmo não havendo lugar a qualquer alteração legislativa que liquide a restrição referida[81], relembramos que a titularidade e direção da investigação cabe à Autoridade judiciária competente em cada fase do processo, cabendo ao Ministério Público (MP), na fase de Inquérito, por imposição constitucional consagrada no n.º 1 do artigo 219.º da CRP, complementada pelo artigo 1.º do Estatuto do Ministério Público (EMP)[82], assumir a competência de *dominus* do inquérito.

Deste modo, possuindo a competência exclusiva para dirigir o inquérito e assegurar as suas finalidades, cabendo aos OPC uma função de coadjuvação e assistência, o MP, na fase de Inquérito[83], pode, na nossa perspetiva delegar a competência de investigação em outro OPC diverso, por considerar que tem as competências e apetências necessárias para prosseguir com as diligências de investigação tidas por convenientes. Atente-se que não desconhecemos o previsto no artigo 8.º da LOIC, em que se prevê que o Procurador-Geral da República pode, também na fase de inquérito, deferir a investigação de um crime a outro OPC quando, em concreto, se lhe afigure mais adequado ao bom andamento da investigação, desde que cumpra os pressupostos previstos nas alíneas do n.º 1 e do n.º 2. Consideramos, antes, que esta possibilidade não invalida a competência natural do específico Magistrado do Inquérito que, enquanto titular do mesmo, tem a faculdade de delegar no OPC que entender o encargo de proceder a diligências e investigações relativas à concreta investigação[84].

---

[81] Embora, como referimos anteriormente, a Informação n.º 20/2010, do DIAP de Lisboa, de 26/04/2010 – Informação da PGDL: crimes cometidos por meios informáticos, embora sem carácter vinculativo, faça já distinção entre crimes informáticos e crimes praticados com recurso a meios informáticos, de menor densidade, podendo, estes últimos, ser investigados por OPC de competência genérica.

[82] Lei n.º 68/2019, de 27 de agosto.

[83] Nos termos do n.º 1 do artigo 262.º do CPP o inquérito, a primeira das fases do processo penal, pretende investigar a verificação de um crime, determinar os seus agentes e a sua responsabilidade, descobrir e recolher provas, para decisão sobre a acusação.

[84] Conforme Artigo 270.º, n.º 1, 3 e 4 do CPP, Artigo 2.º, n.º 2 e 7 da LOIC, Artigo 4.º, n.º 1 al. e) do EMP.

No mesmo sentido do aqui defendido, a nosso ver clarividente, a posição defendida no Acórdão do Tribunal de Relação de Lisboa, relativa ao Processo n.º 50/14.0SLLSB-Y.L1-9, de 06/09/2016, e que embora não se trate de uma decisão com força obrigatória geral, valendo apenas para aquele processo concreto, e bem assim os crimes em investigação se tratarem de outros diferente dos que aqui discutimos, consideramos, *mutais mutandis*, ter devida aplicabilidade, pois a LOIC (…) nunca poderia derrogar disposições legais do CPP e da própria CRP[85].

Ultrapassada esta questão ir-se-iam verificar ganhos visíveis no combate ao cibercrime, cada vez mais sofisticado e organizado, o que deve impelir as autoridades nacionais com competências no combate e investigação do crime em Portugal de garantir que também os OPC se organizem, colaborem e se coordenem entre si.

Quanto à necessária coordenação que deve existir entre os OPC, a LOIC prevê o formato como a mesma se deve verificar, sendo de relevar o artigo 15.º, sob a égide "sistema de coordenação", onde vêm previstas as competências do Secretário-Geral do Sistema de Segurança Interna (SG SSI), que deve nomeadamente, nos termos das orientações genéricas emitidas pelo conselho coordenador, coordenar os OPC, sem prejuízo das competências do MP, entidade competente para dirigir o inquérito, conforme previsto no artigo 263.º, n.º 1 CPP, velar pelo cumprimento da repartição de competências entre OPC de modo a evitar conflitos e garantir a partilha de meios e serviços de apoio de acordo com as necessidades de cada OPC mas, que neste âmbito que vimos discutindo, não parece contribuir, pois não possui competências para tanto, para a solução necessária aos problemas associados ao ciberespaço.

5.3 – Da necessidade de um novo paradigma

Na sociedade moderna é patente a importância exponencial das novas tecnologias, que nos trouxeram desenvolvimento económico, social e cultural, bem como avanço no conhecimento científico, mas que, por outro lado,

[85] Processo n.º 50/14.0SLLSB-Y.L1-9, de 06/09/2016, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8cf93372a59dc58480257fd3004a5256?OpenDocument.

trouxeram-nos também novas e diversas formas de criminalidade complexas e sofisticadas, onde se inclui como preocupante o tráfico de produtos estupefacientes através da *internet*.

Embora as diversas alterações legislativas que o Decreto-Lei n.º 15/93, de 22 de janeiro conheceu desde a sua entrada em vigor, verificamos que o regime, previsto e punido pelo artigo 21.º e seguintes daquele diploma, não prevê especificamente o tráfico de estupefacientes através da *internet*, designadamente através da utilização da *dark web*.

Quanto ao regime de negócios lícitos de compra e venda através da *internet* de superfície, apercebemo-nos, anteriormente, das dificuldades existentes em prevenir atividades ilícitas por ali conduzidas, pois a entidade com competências de supervisão não possui competências que lhe permitam efetuar um verdadeiro patrulhamento cibernético, prevenindo crimes, que amiúde vão ocorrendo através de plataformas *online*, servindo apenas de zelador das atividades dos prestadores de serviços intermédios. Ao mesmo tempo, concluímos da inexistência para estes últimos de um regime sancionatório forte, de tipo penal, podendo lhes apenas ser assacadas responsabilidades ao nível civil e ao nível do mero ordenamento social, com aplicação de eventuais sanções acessórias, nos casos em tenham conhecimento de atividades ilícitas que se desenvolvam através de serviços que oferecem.

Depois, através da análise dos diversos Relatórios Nacionais e Internacionais, bem como Planos de ação concretamente estabelecidos, concluímos que é denominador comum a verificação de que os vários indicadores apontam para uma maior circulação de drogas no mercado da UE e no mercado Nacional numa conjuntura de grandes desafios, como o crescente uso da *internet* na comercialização de diversas substâncias psicoactivas.

Aventam-se recomendações como maior consciencialização para o problema, melhor coordenação nacional e cooperação internacional, bem como se sugere mais cooperação com as entidades privadas, vistas como entidades detentoras de conhecimentos avançados na área das tecnologias, não obstante verificarmos que ao nível da concretização das estratégias definidas são parcos os instrumentos ou planos de ação que objetivem tais exortações.

Considerando, ainda, as dificuldades notórias na prevenção e investigação da criminalidade desenvolvida através da *internet*, julgamos ser pertinente percebermos, em particular, da aplicabilidade do regime previsto na Lei do Cibercrime em prol do combate ao tráfico de estupefacientes por via de plataformas *online*, seja através da denominada *internet* de superfície ou profunda, resposta que demos como positiva. Nessa sequência sobreveio a questão derivada de, considerando a repartição de competências que vigora em Portugal, prevista na LOIC, como rentabilizar a aplicação da referida Lei, contando que a mesma contém um regime processual que conta com meios de obtenção de prova que se revelam de extrema importância tendo em consideração que permitem preservar dados probatórios, no imediato, sob pena de que os mesmos se possam vir a perder, alterar ou deixar de estar disponíveis em linha, cujo acesso se fará no decurso do processo para efeitos de produção de prova.

Em face deste paradigma, concluímos pela necessidade de haver uma alteração legislativa que permita a outros OPC desenvolver a sua atividade investigatória de crimes através da *internet*, considerando a vulgaridade com que esta forma de criminalidade é utilizada pelos criminosos, contando que atualmente a PSP e a GNR detém de formação e conhecimentos técnicos de elevada especialidade, também na área informática, e que em face da notória, porque do conhecimento público, falta de efetivo na PJ, publicamente conhecido, poder-se-iam constituir como fortes aliados no combate a este flagelo.

Não havendo lugar a qualquer alteração legislativa, relembrámos que a titularidade e direção da investigação cabe à Autoridade judiciária competente em cada fase do processo, cabendo ao Ministério Público, que possui a competência exclusiva para dirigir o inquérito e assegurar as suas finalidades, delegar a competência de investigação em outro OPC, diferente do indicado pela LOIC, por considerar que o mesmo tem as competências e valências necessárias para prosseguir com as diligências de investigação tidas por convenientes.

Consideramos ser de extrema importância criar uma estrutura *ex novo*, com funções atribuídas de coordenação nas diversas dimensões da segurança no ciberespaço em Portugal, de modo a se conseguir enfrentar, com

competência e eficácia, as organizações criminosas, cada vez mais sofisticadas e evoluídas. Em alternativa, equacionamos uma maior atuação, ao nível operacional, do CNCS, cuja Autoridade é lhe atribuída pela Estratégia Nacional de Segurança do Ciberespaço, que poderia passar pela coordenação efetiva dos OPC para que os mesmos, depois, em coordenação no âmbito da UCIC Nacional, e com consequente melhor aproveitamento dos canais de cooperação internacional existentes, pudessem executar uma melhor prevenção e combate ao tráfico de estupefacientes através da *internet*.

A criminalidade através da sociedade tecnológica, cujas oportunidades são evidentes, reclama, efectivamente, uma coordenação de outro nível. Seguimos, pois, Luís Elias, quando defende a necessidade de criação de uma estrutura que venha a coordenar as diversas dimensões da segurança no ciberespaço em Portugal, pois só assim será possível enfrentar as organizações criminosas evoluídas, da nova era tecnológica, que "assumem características de grande complexidade, de sofisticação, de pesquisa científica e de desenvolvimento de novas ferramentas tecnológicas, de modi operandi, de novas formas de iludir os sistemas de segurança e os investigadores criminais (…)" (Elias, 2018, p. 343).

Enquanto tal desiderato não se concretiza julgamos ser possível, em desenvolvimento do Eixo 4 (Resposta às ameaças e combate ao Cibercrime) da Estratégia Nacional de Segurança do Ciberespaço [86], consolidar materialmente o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança atribuído ao Centro Nacional de Cibersegurança (CNCS), de forma a que este contribua para as atualizações necessárias à legislação em vigor com vista a suportar as investigações, de modo a poder-se operacionalizar medidas substantivas eficazes de combate ao cibercrime, convocando os OPC de competência genérica (PSP, GNR e PJ [87]) a contribuírem, de forma coordenada, para o combate ao cibercrime, "garantindo que o ciberespaço é [de facto] utilizado como espaço de liberdade, segurança e justiça (…)"[88].

[86] Aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. Disponível em https://dre.pt/dre/detalhe/resolucao-conselho-ministros/92-2019-122498962.
[87] Artigo 3.º, n.º 1 da LOIC.
[88] Disponível em https://www.cncs.gov.pt/sobre-nos/.

Sob a égide estratégica do CNCS, enquanto autoridade nacional, coordenador operacional e especialista em matéria de cibersegurança, poder-se-ia, depois, operacionalizar-se no âmbito da Unidade de Intervenção e Coordenação Conjunta (UCIC[89]) Nacional, julgamos de forma mais eficaz, a constituição de equipas conjuntas com o objetivo de avaliar, decidir e coordenar ações a executar em comum no combate ao tráfico de estupefacientes praticado através da *internet*, concorrendo ambos os OPC para uma precoce deteção de atividades desta natureza, por exemplo através de ciber patrulhas desenvolvidas em conjunto no ciberespaço, de prevenção, sinalização e monitorização de crimes de tráfico de estupefacientes *online*, vislumbrando-se o aproveitamento e comunhão de esforços de todos em prol de um fim último que todos nós procuramos: uma sociedade mais (ciber)segura.

Cremos que, deste modo, alcançaríamos uma melhor cooperação policial interna, entre os OPC, e em consequência conseguir-se-ia uma melhor cooperação policial internacional, consubstanciada outrossim como prioridade estratégica (n.º 9) a prosseguir pelas Autoridades competentes dos Estados-Membros no âmbito do Plano de Ação da União Europeia em matéria de drogas 2021-2025, conseguindo-se um melhor diálogo e partilha de informações, seguindo os padrões europeus definidos e adotados nos diversos países da UE, com utilização mais eficiente das valências disponibilizadas pela EUROPOL, nomeadamente no acesso à sua base de dados, providenciando *analysis & checking of data* em tempo real, o que atualmente ainda não sucede com a ocorrência desejável, quiçá por via dos problemas de coordenação que ainda subsistem entre as polícias nacionais, pelo que encaramos como urgente que os canais de cooperação policial neste âmbito, tanto nacionais como internacionais, sejam aperfeiçoados, com clara melhoria na troca de informações, com o objetivo de detetar, prevenir e combater precocemente atividades de tráfico de estupefacientes desenvolvidas através da *internet*.

[89] Através de Protocolo firmado entre os órgãos de polícia criminal e serviços aduaneiros e de segurança foram criadas seis UCIC – Lisboa, Norte, Sul, Centro, Madeira e Açores, por forma a garantir uma eficiente e célere troca de informação entre órgãos e serviços empenhados no combate ao tráfico de droga, dando escopo ao Decreto-lei n.º 81/95, de 22 de abril.

Em complemento, cremos que a PSP deve desenvolver uma estrutura sólida, ao nível de Divisão[90], inserida no Departamento de Investigação Criminal, apetrechada de meios tecnológicos necessários que lhe permita desenvolver atividades de prevenção, com sinalização e monitorização de atividades de tráfico de substâncias estupefacientes *online*, coordenando subsequentes investigações, delegadas pela Autoridade Judiciária competente, que corram termos nos diversos Comandos Territoriais, pois o "eixo de combate ao cibercrime compreende o conjunto de iniciativas de actualização e de harmonização legislativa com vista a uma mais eficaz (…) capacitação dos órgãos de polícia criminal (…) na prossecução dos seus objectivos no ciberespaço" (Santos, 2018, p. 28).

5.4 – Conclusão capitular

Concluímos anteriormente que o crime de tráfico de estupefacientes através da internet pode, e deve, ser investigado pela PSP, enquanto OPC de competência genérica. Com utilização de meios informáticos, ou necessariamente pela utilidade da obtenção de prova em meios digitais ou suportes eletrónicos, as disposições materiais e processuais ínsitas na Lei do cibercrime têm aplicabilidade, *tout court*, à investigação de crimes de tráfico de estupefacientes através da internet ou com utilização de meios de comunicação *online*.

Por seu turno, a LOIC prevê que os crimes informáticos e praticados com recurso a tecnologia informática são da competência reservada de investigação da PJ (artigo 7.º n.º 3, al. l), mas que, sustentados nos capítulos anteriores, notamos que tal restrição é de tal modo anacrónica, que se baseia numa repartição de competências entre OPC rígida operada em 2008, que perante o desenvolvimento da investigação criminal em Portugal, e investimento que tem sido injetado noutros OPC, designadamente na formação e empenho ativo da PSP, não mais sentido faz, até porque atualmente as tendências demonstram-nos que a criminalidade organizada moderna sustenta a sua atividade nos benefícios da internet, em especial da darknet.

[90] Criação da Divisão de Coordenação de Cibercriminalidade.

Ainda que sem alteração legislativa que aniquile o óbice referido, consideramos que, em última análise, a titularidade do inquérito cabe à Autoridade judiciária competente, neste caso MP, podendo a competência de investigação de crimes informáticos ser delegada noutros OPC diferentes da PJ, desde que detenham a competência e apetência necessária para prosseguir a investigação, tal como a PSP possui, verificando-se ganhos visíveis no combate ao cibercrime, cada vez mais sofisticado e organizado.

Neste contexto, considerámos como proposta viável, mas ainda em amadurecimento, que a PSP, enquanto polícia integral, moderna e evoluída, deverá desenvolver uma estrutura orgânica sólida, em desenvolvimento do já criado Núcleo de Cibercriminalidade do Departamento de Investigação Criminal, que opere a nível de divisão, apetrechada de meios tecnológicos necessários que lhe permita desenvolver atividades de prevenção (patrulhamento cibernético), de modo a sinalizar precocemente atividades de tráfico de substâncias estupefacientes e outros crimes que se desenvolvam em ambiente *online*, com meios necessários que permita, igualmente, apoiar investigação em curso ou que venham a decorrer no seio da PSP.

Ainda assim, relevamos importante a criação em Portugal de uma estrutura *ex novo*, com atribuição de competências de coordenação nas diversas dimensões da segurança no ciberespaço ou, em alternativa, garantir uma atuação real e operacional do CNCS (Eixo 4 da Estratégia Nacional de Segurança do Ciberespaço), que poderia passar pela coordenação efetiva dos OPC, de modo que os mesmos pudessem executar, em conjunto, uma melhor prevenção e combate ao tráfico de estupefacientes através da internet, o que poderia ocorrer até junto de estruturas anteriormente criadas, que objetivam a coordenação entre OPC do tráfico de estupefacientes (UCIC).

CONCLUSÃO

A criminalidade organizada transnacional, no mundo global em que vivemos, não conhece hoje fronteiras físicas nem tecnológicas, tendo vindo a prosperar entre nós, operando a partir de diversos países, mas com incidência noutros, tornando complexo e de difícil deteção as atividades que prosperam entre os grupos organizados de criminosos, em especial os cibercriminosos, contando com a sua atuação anónima e confidencial, através de plataformas *online* encriptadas.

Ao longo do nosso trabalho demonstramos patente preocupação com a cibercriminalidade, máxime cibertráfico, considerando que as organizações criminosas modernas fazem mister a utilização de plataformas *online* e comunicações *end-to-end*, encriptadas, no desenvolvimento da sua atividade criminosa, exigindo um esforço atualista da atividade das forças policiais, em ordem a conseguir detetar precocemente os crimes praticados através da internet, ao mesmo tempo que se lhes exige uma atuação preventiva, a fim de impossibilitar a sua ocorrência.

Neste âmbito, consideramos importante dar enfâse à necessidade de se garantir uma coordenação policial interna entre os OPC eficaz, relevando a possibilidade de criação de um ponto único de contato para a coordenação policial interna, de modo a garantir uma eficiente interoperabilidade entre OPC no combate à criminalidade organizada.

Garantida que fica a correta coordenação interna e operacional de investigações, verificar-se-ia uma melhor utilização dos canais de cooperação policial internacional, beneficiando todos os OPC de informação útil e oportuna aos seus processos em investigação, provenientes dos diversos canais de cooperação policial internacional, funcionalmente geridos pelo PUC-CPI, funcionando de forma fluída, acrescentando valor às investigações criminais que decorrem nos diferentes OPC, de modo a contribuir para a luta contra a criminalidade organizada transnacional existente, cujo interesse é nacional.

Cremos, portanto, ser de extrema importância que, para haver uma melhor cooperação policial internacional no combate à cibercriminalidade organizada – cibertráfico, por exemplo – deverá primeiro haver a montante uma melhor e eficiente cooperação e coordenação interna, pelo que encaramos

como urgente que os canais de cooperação policial, tanto nacionais como internacionais, sejam aperfeiçoados, com clara melhoria na troca de informações, com o objetivo de identificar precocemente os movimentos dos grupos organizados de criminosos transnacionais, contribuindo para uma melhor segurança interna nacional, permitindo a todos os OPC, sem exceção, aceder oportuna e utilmente a informação proveniente da EC3 e da EU *Innovation Hub*.

Questionamos (pergunta de partida), acerca da aplicabilidade da Lei do cibercrime ao crime de tráfico de estupefacientes através da internet, concluindo na positiva, considerando que o traficante moderno, altamente organizado e evoluído, como vimos, não dispensa a utilização de comunicações digitais para desenvolver as suas atividades de tráfico ilícito com sucesso, ou necessariamente pela utilidade da obtenção de prova em meios digitais ou suportes eletrónicos, as disposições materiais e processuais têm aplicabilidade, *tout court*, à investigação de crimes de tráfico de estupefacientes através da internet ou co utilização de meios de comunicação online.

A evolução das tecnologias de informação e comunicação tem sido exponencial. As organizações criminosas recorrem hoje, mais do que nunca, a estas novas ferramentas para aumentar os seus lucros, para conseguirem o anonimato, para obterem uma maior eficiência e eficácia nas suas operações ilícitas e para conseguirem escapar à ação da justiça e das polícias. Neste sentido, a lei também tem de se adaptar aos novos tempos, sendo incompatível a manutenção de cláusulas de exclusividade de investigação para um OPC (PJ) em detrimento de outros, quando hoje a utilização destas tecnologias emergentes é massiva por parte dos cidadãos e dos criminosos.

Neste patamar, relativamente à questão derivada que levantamos no nosso estudo, de saber como articular a aplicabilidade da Lei do Cibercrime ao crime de tráfico *online*, considerando o quadro atual de repartição de competências de investigação acometidas aos OPC em Portugal, após revisitarmos a LOIC, considerámos que, em face da evolução tecnológica e do aproveitamento das virtualidades da internet e das novas formas de comunicação *online* por parte dos cibercriminosos, urge efetuar-se uma revisão legislativa no sentido de os crimes praticados através de meios informáticos ou com recurso a tecnologia informática, que atualmente se inserem na

competência reservada de investigação da PJ, passem formalmente para a competência de investigação de OPC de competência genérica.

Se é certo que, em última análise, quem define as competências de investigação é o Ministério Público, Autoridade Judiciária a quem compete a titularidade do inquérito, a verdade é que o arquétipo legal previsto na LOIC, por falta de clareza, dificulta a ação investigatória de outros OPC, designadamente da PSP, quando ativamente colha notícias de crimes de tráfico *online* de estupefacientes, ou por exemplo, de tráfico de artigos pirotécnicos por parte dos grupos organizados de adeptos, obstaculizando a possibilidade de fazer uso dos meios processuais previstos na Lei do cibercrime, urgindo revisão e atualização legal da Lei de organização de investigação criminal.

Colhendo acolhimento do presente argumento, consideramos que ficarão preenchidas as condições para uma melhor prevenção e combate ao tráfico de estupefacientes com recurso a novas tecnologias, contando com concomitante modernização tecnológica e eventual atualização funcional das atribuições do Departamento de Investigação Criminal da PSP, de forma a capacitá-lo a acompanhar outras polícias modernas e evoluídas, indo de encontro à satisfação dos anseios das entidades públicas competentes nacionais e internacionais, transpostos nos relatórios que plasmamos no nosso trabalho.

Por fim, relevamos de extrema importância o papel a desempenhar pelo centro nacional de cibersegurança, pelos serviços informações de segurança, bem como das forças de segurança que deverão trabalhar em permanente coordenação e com partilha de informação, de modo a detetar precocemente atividades que possam indiciar a prática de crimes altamente organizados, alinhados que estejam com as estratégias europeia e nacional de luta contra o tráfico de estupefacientes, como vimos objetivo premente enunciado no Plano de Ação da UE em matéria de drogas 2021-2025, exigindo-se uma forte aposta nos serviços de prevenção, designadamente da PSP, acompanhando os mercados de droga na internet visível e oculta, de forma a travar os mercados de drogas ilícitas de base digital.

REFERÊNCIAS BIBLIOGRÁFICAS

Anes, F. (2015). Criminalidade Transnacional e Globalização. In Bacelar, J. & Santos, S. (coord.), *Enciclopédia de Direito e Segurança* (89-94). Almedina.

Azevedo, D. (2016). *Tráfico de droga pela internet – Tentativa de enquadramento jurídico* (Dissertação de Mestrado). Universidade do Minho – Escola de Direito.

Bardin, L. (2020). *Análise de conteúdo*. Edições 70.

Brandão, Ana Paula (2011), Dinâmicas Transnacionais e Securitizadoras: O Efeito Amplificador, Brandão, A et al., A Luta contra o Terrorismo Transnacional: Contributos para uma reflexão, Almedina.

Braz, J. (2004). A cooperação internacional na luta contra o tráfico de droga. *Separata da Faculdade de Direito da Universidade de Lisboa* (173-200). Coimbra editora.

Campenhoudt, L., Marquet, J., & Quivy, R. (2019). *Manual de investigação em ciências sociais*. Gradiva.

Campos, J. & Campos, J. (2010). *Manual de Direito Europeu. O Sistema institucional, a ordem jurídica e o ordenamento económico da União Europeia*. (6.º ed.). Coimbra Editora.

Cruz, R. (2021). *A Criminalidade Organizada Itinerante – Identificação e Combate no Ponto de Origem* (Trabalho da UC – Teoria e Prática Policial). ISCPSI.

Correia, E. & Dias, F. (2000). *Direito Criminal*. Livraria Almedina.

Craveiro, R. (2019). *As Equipas de Investigação Conjunta da União Europeia como instrumento de investigação criminal* (Dissertação de Mestrado). Academia Militar.

Davin, J. (2007). *A Criminalidade Organizada Transnacional. A cooperação Judiciária e Policial na UE* (2.ª edição – revista e aumentada). Almedina.

Elias, L. (2011). *Segurança na Contemporaneidade – Internacionalização e Comunitarização* (Tese de Doutoramento). Faculdade de Ciências Sociais e Humanas – Universidade Nova de Lisboa.

Elias, L. (2018). *Ciências Policiais e Segurança Interna. Desafios e Prospetiva, Lisboa.* ISCPSI-ICPOL.

Fernandes, P. (2013). *A Naturaleza e o Homem: Da contemplação à Instrumentalização dos Antigos Gregos a uma Sociedade de Riscos* (Tese de Doutoramento). Universidade de Salamanca.

Ferreira, J. (2018). *Compra de drogas pela Internet* (Trabalho final de Licenciatura). Faculdade de Ciências Humanas e Sociais. Universidade Fernando Pessoa.

Giddens, A. (2000). *O mundo na era da globalização*. Presença.

Lakatos, E. M., & Marconi, M. A. (2003). *Fundamentos de metodologia científica* (5.ª ed.) Editora Atlas.

Lourenço, N. (2015). Criminalidade Transnacional e Globalização. In Bacelar, J. & Santos, S. (coord.). *Enciclopédia de Direito e Segurança* (94-96). Almedina.

Moniz, P. (2018). Impacto do Ciberespaço na Sociedade em Rede. In Nunes, P. (coord.). *Contributos para uma estratégia nacional de ciberdefesa* (28) (17-24). IDN

Macedo, J. (2009). *Algumas considerações acerca dos crimes informáticos em Portugal, Direito Penal Hoje – Novos desafios e novas respostas*. Coimbra Editora.

Nunes, D. (2021). *Os meios de obtenção de prova previstos na Lei do cibercrime*. Gestlegal.

Prates, D. (2011). Conclusões do Seminário “Crime sem Fronteiras”. In *Revista do Instituto Superior de Ciências Policiais e Segurança Interna* (191-197). Politeia.

Ramalho, D. (2013). A investigação criminal na darkweb. Revista de concorrência e regulação. Ano IV – Número 14/15 Abril/Setembro 2013. Instituto de Direito Económico Financeiro e Fiscal da Faculdade de Direito da Universidade de Lisboa.

Ramos, A. (2022). O Agente encoberto digital – meios especiais e técnicos de investigação criminal. Almedina.

Rodrigues, A. (2009). Criminalidade Organizada – Que política criminal. In *Direito Penal Económico e Europe*u: Textos doutrinários vol. III (191). Coimbra Editora.

Santos, A. F. C. (2015). *O cibercrime: Desafios e respostas do direito* (Mestrado em Direito). Universidade Autónoma de Lisboa.

Santos, L. (2018). Segurança do ciberespaço. In Nunes, P. (coord.). *Contributos para uma estratégia nacional de ciberdefesa.* (28). (25-31). IDN.

Sousa, A. (2001). *Separata de Estudos em Comemoração – por cinco anos (1995-2000) da Faculdade de Direito da Universidade do Porto*. Coimbra Editora.

Valente, M. (2019). *Teoria Geral do Direito Policial* (6.º ed.). Almedina.

Valente, M. (2009). A investigação do crime organizado, Buscas domiciliárias nocturnas, o agente infiltrado e intervenção nas comunicações. In *Criminalidade organizada e criminalidade de massa – Interferências e ingerências mútuas* (161). Almedina.

Verdelho, P. (2006). A convenção sobre cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa. In *Direito da Sociedade de Informação* Vol. VI. (257-277). Coimbra Editora.

Verdelho, P., Bravo, R. & Rocha, M. (2003). *Leis do Cibercrime*. V. 1 (1.º ed.). Centroatlantico.pt.

LEGISLAÇÃO CONSULTADA

Convenção das Nações Unidas Contra a Criminalidade Organizada [Convenção de Palermo], (2000). Retirado de: http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_nu_criminalidade_organizada_transnacional.pdf.

Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas - Assinada e ratificada internamente através da Resolução da Assembleia da República n.º 29/91 e Decreto do Presidente da República n.º 45/91, publicados no Diário da República, de 6 de setembro de 1991.

Convenção de Aplicação do Acordo de Schengen, (1985). Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A42000A0922%2802%29.

Decisão 2007/533/JAI do Conselho (2007) e Regulamento (CE) N.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de Dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SISII)

Decreto n.º 13/2007, de 13 de junho – Acordo entre a República Portuguesa e o Reino de Espanha sobre a Cooperação transfronteiriça em matéria de cooperação policial e aduaneira. https://dre.pt/home/-/dre/636066/details/maximized.

Decreto de 10 de abril de 1976 – Constituição da República Portuguesa

Decreto-Lei n.º 78/87, de 17 de fevereiro, atualizado até à Lei n.º 39/2020, de 18 de agosto – Código de Processo Penal

Decreto-Lei n.º 81/95, de 22 de abril – Prevê a criação de brigadas anticrime e de unidades mistas de coordenação integrando a Polícia Judiciária, a Guarda Nacional Republicana, a Polícia de Segurança Pública, o Serviço de Estrangeiros e Fronteiras e a Direcção-Geral das Alfândegas

Decreto-Lei n.º 49/2017, de 24 de maio – Cria o Ponto Único de Contacto para a Cooperação Policial Internacional

Decreto-Lei n.º 137/2019, de 13 de setembro – Aprova a nova estrutura organizacional da Polícia Judiciária

Decreto-Lei n.º 10/2020, de 11/03 – Estabelece a orgânica do Ponto Único de Contacto para a Cooperação Policial Internacional (revoga o Decreto Regulamentar n.º 7/2017, de 7 de agosto).

Decreto-Lei n.º 24/2014, de 14 de fevereiro – Contratos celebrados à distância e fora do estabelecimento comercial.

Decreto-Lei n.º 48/95, de 15 de março, actualizado até à Lei n.º 94/2021, de 21 de dezembro – Código Penal

Decreto-Lei n.º 78/87, de 17 de fevereiro, actualizado até à Lei n.º 13/2022, de 01 de agosto – Código de Processo Penal.

Decreto-Lei n.º 15/93, de 22 de janeiro – Legislação de Combate à Droga.

Decreto-Lei n.º 7/2004, de 7 de janeiro – Regime de negócios lícitos de compra e venda através da internet.

Decreto Regulamentar n.º 7/2017, de 7 de agosto – Estabelece a organização e o funcionamento do Ponto Único de Contato para a Cooperação Policial Internacional

Documento 9798/15, de 10 de junho de 2015, JAI 442 COSI 67 – Projeto de conclusões do Conselho sobre a Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020

Documento 10492/14, de 13 de junho de 2014, DAPIX 75 ENFOPOL 157 – Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information Exchange

Lei n.º 68/2019, de 27 de agosto – Estatuto do Ministério Público.

Lei n.º 17/2016, de 23 de maio – Lei Quadro-política criminal.

Lei n.º 49/2008, de 27 de agosto, atualizada até à Lei n.º 57/2015, de 23/06 – Lei de Organização da Investigação Criminal.

Lei n.º 53/2008, de 29 de agosto, atualizada até à Lei n.º 21/2019, de 25/02 – Lei de Segurança Interna.

Lei n.º 73/2009, de 12 agosto, atualizada até à Lei n.º 38/2015, de 11 de maio – Estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos OPC.

Lei n.º 74/2009, de 12 de agosto, o regime aplicável ao intercâmbio de dados e informações de natureza criminal entre as autoridades dos Estados membros da União Europeia, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2006/960/JAI, do Conselho, de 18 de dezembro

Lei n.º 67/98, de 26 de outubro – Lei da Proteção de Dados Pessoais.

Lei n.º 109/2009, de 15 de setembro, actualizada até à Lei n.º 79/2021, de 24 de novembro – Lei do Cibercrime.

Lei n.º 55/2020, de 27/08 – Lei de Política Criminal – Biénio 2020-2022.

Lei n.º 101/2001, de 25 de agosto – Regime jurídico das ações encobertas para fins de prevenção e investigação criminal.

Portaria n.º 1354/2008, de 27/11 – Aprova o Regulamento de funcionamento dos Centros de Cooperação Policial e Aduaneira entre a República Portuguesa e o Reino de Espanha, https://dre.pt/pesquisa/-/search/440572/details/maximized.

Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho (2006). Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32006R0562.

Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial

Regulamento (CE) n.º 810/2009, do Parlamento Europeu e do Conselho (2009). Retirado de https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32009R0810.

Regulamento 1987/2006 do Parlamento e do Conselho (2006). Retirado de https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32006R1987.

JURISPRUDÊNCIA CONSULTADA

Acórdão do TRP 01.12.2017, disponível em:
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/a9b57564fd92e3e980258218005302bc?OpenDocument.

Acórdão do TRL - Processo n.º 50/14.0SLLSB-Y.L1-9, de 06/09/2016.

ESTRATÉGIAS / PROGRAMAS / RELATÓRIOS / PLANOS (NACIONAIS E INTERNACIONAIS)

Estratégia Nacional de Luta contra a Droga - Aprovada pela Resolução do Conselho de Ministros n.º 46/99, de 26 de maio.

Estratégia da UE de Luta conta a Droga (2021-2025).

Estratégia da UE para a União da Segurança para 2020-2025.

Estratégia Nacional de Segurança do Ciberespaço - Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho.

European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

Gabinete de cibercrime da Procuradoria-geral da República (2022). Nota informativa, de 13 de julho de 2022, relativo às denúncias de cibercrime recebidas, electronicamente, no 1.º semestre de 2022

Plano de Atividades 2021-2023 da EUROPOL

Plano Nacional para a redução dos Comportamentos Aditivos e das Dependências, 2013-2020.

Plano de Ação da União Europeia em matéria de drogas 2021-2025.

IV Inquérito nacional ao consumo de substâncias psicoativas na população geral (INPG) – 2016/17.

Programa do XXII Governo Constitucional de Portugal, 2019-2023.

Protocolo de Coordenação UCIC – 1996.

Relatório Anual de Segurança Interna, 2020.

Relatório Anual de Segurança Interna, 2021.

Relatório Anual do SICAD (2019). A situação em Matéria de Drogas e Toxicodependências.

Relatório Europeu sobre Drogas. Tendências e evoluções, 2021 - Observatório Europeu da Droga e da Toxicodependência (2021), Relatório Europeu sobre Drogas 2021: Tendências e Evoluções, Serviço das Publicações da União Europeia, Luxemburgo.

Serious and Organised Crime Threat Assessment, 2021.

SITES CONSULTADOS

https://www.techadvisor.com/article/727316/what-is-the-dark-web-whats-on-it-how-to-access-it.html.

https://pplware.sapo.pt/informacao/deep-web-o-o-lado-obscuro-da-internet/.

https://www.portugal.gov.pt/gc22/programa-do-governo-xxii/programa-do-governo-xxii-pdf.aspx?v=%C2%ABmlkvi%C2%BB=54f1146c-05ee-4f3a-be5c-b10f524d8cec.

http://www.sicad.pt/BK/Publicacoes/Lists/SICAD_PUBLICACOES/Attachments/71/ENresolucao.pdf.

http://www.sicad.pt/BK/Institucional/Coordenacao/Documents/Planos/SICAD_Plano_Nacional_Reducao_CAD_2013-2020.pdf.

http://www.sicad.pt/BK/Publicacoes/Lists/SICAD_PUBLICACOES/Attachments/169/Relatorio_Anual_2019_A_SituacaoDoPaisEmMateriaDeDrogas_e_Toxicodependencias.pdf.

https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet_en.

https://www.europol.europa.eu/publications-documents/europol-programming-document.

https://www.emcdda.europa.eu/system/files/publications/13838/2021.2256_PT_03.pdf.

https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

https://www.europol.europa.eu/publications-documents/europol-programming-document.

https://www.consilium.europa.eu/pt/press/press-releases/2020/12/18/council-approves-the-eu-drugs-strategy-for-2021-2025/.

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

http://www.sicad.min-saude.pt/pt/Paginas/detalhe.aspx?itemId=560&lista=SICAD_NOVIDADES&bkUrl=/BK.

http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8cf93372a59dc58480257fd3004a5256?OpenDocument.

https://dre.pt/home/-/dre/67468089/details/maximized.

https://www.cncs.gov.pt/sobre-nos/.

https://www.europol.europa.eu/keywords/eu-police-cycle-empact (EMPACT).

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002F0465 (Equipas de Investigação Conjuntas).

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0794 (EUROPOL).

https://frontex.europa.eu/media-centre/news-release/frontex-welcomes-new-standing-corps-recruits-ILr9os (FRONTEX, criação de standing corps).

https://www.interpol.int/en/Who-we-are/What-is-INTERPOL (INTERPOL).

https://www.portugal.gov.pt/gc22/programa-do-governo-xxii/programa-do-governo-xxii-pdf.aspx?v=%C2%ABmlkvi%C2%BB=54f1146c-05ee-4f3a-be5c-b10f524d8cec (Programa do XXII Governo Constitucional de Portugal (2019)).

https://europa.eu/european-union/about-eu/countries/member-countries/portugal_pt (Relatório do Global Peace Index (2020)).

https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABAAzNzU0AwBUqv9nBAAAAA%3d%3d (RASI, 2018).

https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDA0sAAAQJ%2bleAUAAAA%3d (RASI, 2019).

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14544 (Sistema de Informação Schengen II).

https://www.consilium.europa.eu/pt/policies/eu-fight-against-organised-crime-2018-2021/.

https://www.consilium.europa.eu/pt/council-eu/preparatory-bodies/standing-committee-operational-cooperation-internal-security/.

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656042/IPOL_STU(2020)656042_EN.pdf.

https://popcenter.asu.edu/content/25-techniques.

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0794, acedido em 24/12/2020.

https://www.interpol.int/en/Who-we-are/What-is-INTERPOL (INTERPOL).