INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

**VI CURSO DE COMANDO E DIREÇÃO POLICIAL**

Trabalho Individual Final

# O Impacto da Cibercriminalidade na Atuação Policial: Desafios e Respostas


Auditor

**Tiago Filipe Teixeira da Silva**


Lisboa, 17 de outubro de 2025

## Resumo

O presente trabalho analisou de forma aprofundada os impactos da cibercriminalidade na atuação policial contemporânea, evidenciando a necessidade de reconfiguração institucional, tecnológica e formativa das forças de segurança, em particular da Polícia de Segurança Pública. Demonstrou-se que a crescente sofisticação e transnacionalidade dos crimes digitais colocam desafios significativos às estruturas tradicionais de policiamento, exigindo uma abordagem integrada que articulasse inovação tecnológica, formação especializada e atualização legislativa. Verificou-se que a assimetria entre as capacidades tecnológicas dos cibercriminosos e os recursos disponíveis nas polícias compromete a eficácia da resposta operacional. O estudo concluiu que o desenvolvimento de competências digitais e a criação de ecossistemas de cooperação internacional constituem fatores decisivos para a construção de um modelo de policiamento digital mais eficiente, ético e democrático. A análise revelou ainda que a adequação normativa, aliada à formação contínua e à interoperabilidade técnica, se apresenta como condição essencial para reforçar a resiliência institucional e a proteção dos direitos fundamentais.

O trabalho permitiu, assim, sustentar a necessidade de um novo paradigma de ciberpoliciamento, capaz de assegurar uma resposta preventiva e proativa perante as ameaças emergentes do ciberespaço.


*Palavras-chave:* Cibercriminalidade; Cooperação Internacional; Formação Policial; Policiamento Digital; Tecnologia.

## Abstract

This study thoroughly analyzed the impacts of cybercrime on contemporary police activity, highlighting the need for institutional, technological, and training reconfiguration within law enforcement agencies, particularly the Public Security Police. It demonstrated that the increasing sophistication and transnational nature of digital crimes bring along significant challenges to traditional policing structures, requiring an integrated approach combining technological innovation, specialized training, and legislative adaptation. It was found that the asymmetry between the technological capacities of cybercriminals and the resources available to police officers compromises the effectiveness of operational responses. The study concluded that the development of digital competences and the establishment of international cooperation ecosystems were decisive factors in building a more efficient, ethical, and democratic model of digital policing. The analysis further revealed that regulatory adequacy, together with continuous training and technical interoperability, constituted essential conditions for strengthening institutional resilience and protecting fundamental rights.

This research allowed to support the need for a new paradigm of cyber policing capable of ensuring a preventive and proactive response to emerging threats in cyberspace.


*Keywords:* Cybercrime; Digital Policing; International Cooperation; Police Training; Technology.

# Índice

# Introdução

"A história da Internet pode ser relativamente curta, mas é difícil pensar em outra tecnologia que tenha tido um impacto tão dramático no lazer, nos prazeres e na vida profissional de tantas pessoas, pelo menos desde que Henry Ford introduziu a tecnologia produzida em massa nos carros a motor há um século atrás" (Jewkes &Yar, 2010). De igual forma, "a Internet e as redes sociais, representam um novo cenário para a atividade da criminalidade organizada, muito por conta do fácil acesso à informação (Elias, 2019). Na mesma ótica, a transformação digital tem vindo a redefinir de forma profunda as estruturas sociais, económicas e institucionais em todo o mundo, gerando benefícios significativos, mas também novos riscos e ameaças. Entre estas, destaca-se a cibercriminalidade, uma forma de criminalidade transnacional, desmaterializada e em rápida mutação, que representa um dos maiores desafios contemporâneos à segurança pública e à atuação das forças policiais (Lesmana et al., 2023; Saeed et al., 2023).

O presente trabalho tem como objetivo compreender os impactos crescentes da cibercriminalidade na atuação policial, procurando responder às seguintes questões orientadoras: Quais são os principais desafios que a cibercriminalidade coloca à atuação policial? Que estratégias podem ser implementadas para melhorar essa resposta?

Para a elaboração do presente trabalho, recorreu-se a uma metodologia de natureza iminentemente teórica, assente na análise de estudos científicos, na consulta da legislação aplicável e na apreciação de relatórios de âmbito nacional e internacional.

A pertinência deste tema, justifica-se pela escalada de incidentes cibernéticos nos últimos anos, tanto em número como em sofisticação. Recentemente, a Europol identificou a cibercriminalidade como uma das cinco maiores ameaças à segurança da União Europeia (UE), com destaque para os ataques de *ransomware,* a exploração de dados pessoais e o cibercrime financeiro (EUROPOL, 2025). Em Portugal, foi registado um aumento significativo de denúncias de crimes informáticos, com impacto direto sobre empresas, cidadãos e instituições públicas (Alves, 2025).

Neste contexto, as forças policiais, na qual está, obviamente, a Polícia de Segurança Pública (PSP), enfrentam um duplo desafio: por um lado, adaptar-se tecnicamente à complexidade dos crimes cometidos em ambiente digital; por outro, desenvolver estratégias de prevenção, de investigação e de cooperação internacional que permitam uma atuação eficaz num espaço marcado pela volatilidade tecnológica e pela ausência de fronteiras físicas (Cucoreanu, 2024).

Deste modo, o trabalho assume uma relevância acrescida, não apenas pela atualidade do tema, mas também pelo seu impacto direto na eficácia das polícias, na proteção dos direitos fundamentais e no reforço da confiança dos cidadãos no Estado de Direito. Pretende-se, igualmente, contribuir para o debate académico e efetuar uma reflexão institucional no que toca à articulação entre inovação tecnológica, formação e resposta integrada no combate à cibercriminalidade.

# 1. Estado da Arte

## 1.1. A Emergência e Contextualização Teórica da Cibercriminalidade

A cibercriminalidade constitui uma das maiores ameaças à segurança pública global, exigindo respostas cada vez mais especializadas das forças policiais (Allahrakha, 2024). O termo abrange um conjunto vasto de delitos cometidos com recurso a tecnologias digitais, desde fraudes eletrónicas e *ciberbullying* até ataques a infraestruturas críticas por meio de *ransomware* (European Union Agency for Cibersecurity [ENISA], 2024). Em Portugal, os autores Garcia Marques e Lourenço Martins (2006) foram os primeiros a abordarem o conceito de cibercriminalidade, definindo-o "como todo o acto em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo simbólico desse acto ou em que o computador é objecto do crime". Ou seja, começou a ser "uma ameaça crescente para os direitos fundamentais dos cidadãos" (Elias, 2018). Luís Elias (2019) define-a "como toda e qualquer prática criminosa que tenha associada à sua realização, ou como meio, um aspeto cibernético ou a utilização de computadores". De igual modo, Pedro Dias Venâncio (2021) define a cibercriminalidade como aquela "em que o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objeto de proteção". Ou seja, abrange não apenas a criminalidade, cujo bem jurídico protegido reside no acesso ou na funcionalidade dos sistemas de informação, mas igualmente toda criminalidade em que a informática se apresenta como elemento indispensável para a sua consumação. Deste modo, verifica-se que a sua crescente sofisticação é impulsionada por fatores como a globalização da internet, a proliferação de dispositivos conectados e a acessibilidade de ferramentas de *hacking*, muitas vezes disponíveis na *dark web* (Whelan et al., 2023).

A digitalização generalizada da vida social e económica aumentou, exponencialmente, os vetores de ataque. Veja-se que já em 2011, Pedro Venâncio estruturou a cibercriminalidade em dois grandes vetores. O primeiro são as ofensas focadas

no computador, ou seja, são ofensas que só passaram a existir após o surgimento da Internet. O segundo vetor são as ofensas assistidas pelo computador, que são entendidas como aquelas que já existiam antes da era da Internet, mas que ganharam uma nova vida, ou seja, passaram a ser muito mais executadas através da informática. Isto é, são crimes que são praticados através da Internet, todavia, podem continuar a ser cometidos com a sua ausência. Numa publicação mais recente, David Wall (2017), consagrou um terceiro vetor, além dos dois já citados, designando-o por ofensas *ciberfacilitadas*, ou seja, correspondem a crimes já praticados tradicionalmente, mas pela facilidade proporcionada pela utilização da Internet, o seu cometimento é muito mais eficaz. Dito de outro modo, como aponta Meulebroucke et al. (2025), o espaço virtual tornou-se uma nova arena para o exercício do poder, onde o crime assume formas invisíveis, transnacionais e altamente voláteis. Luís Elias (2019) refere que o "ambiente virtual ao nível global é utilizado para os mais diversos efeitos: para lazer; para a troca e partilha de conhecimento no meio académico e científico ou técnico; (…) e para a prática de uma vasta panóplia de crimes". Esta forma de crime, onde muitas vezes não há um rosto, é potenciado em virtude destas tecnologias "estarem a ser introduzidas e desenvolverem-se muito mais rapidamente do que os legisladores e as agências de aplicação da lei podem reagir" (Klymenko et al., 2020), criando assim um sério desafio às formas tradicionais de policiamento, levantando dilemas éticos, técnicos e legais que exigem uma profunda reconfiguração institucional.

Os dados estatísticos mais recentes evidenciam a tendência de uma subida gradual de crimes perpetrados por cibercriminosos. Segundo o Internet Crime Report do Federal Bureau of Investigation (FBI, 2025), só em 2024 foram registadas mais de 850 mil queixas de cibercrime nos Estados Unidos da América (EUA), representando perdas superiores a 16 mil milhões de dólares. Na União Europeia, o Report on the State of cybersecurity in the Union da ENISA (2025) identificou o *phishing*, o *ransomware* e o comprometimento de dados como as ameaças mais recorrentes, com impacto direto em cidadãos, empresas e organismos públicos. Em Portugal, o panorama tem seguido uma trajetória igualmente preocupante. De acordo com o Relatório Anual de Segurança Interna (RASI, 2024), no pretérito ano, foram registadas cerca de 2500 ocorrências de cibercrime, verificando-se que desde 2015 a criminalidade informática tem vindo a aumentar progressivamente, havendo um aumento colossal desta criminalidade participada, de 48.3%, pós pandemia Covid-19. Na sua dimensão civil, o Centro Nacional de Cibersegurança (CNCS) tem reforçado a necessidade de literacia digital e de uma estratégia nacional articulada de ciberdefesa, apontando falhas na articulação entre entidades civis e forças policiais (CNCS, 2025).

Este cenário evidencia a transição do crime para o ciberespaço, onde a velocidade, anonimato e desmaterialização dificultam a deteção e a investigação. A emergência da cibercriminalidade, com as suas múltiplas camadas técnicas, sociais e jurídicas, exige das forças policiais uma reconfiguração profunda das suas competências, da qualificação tecnológica e da formação. Ao mesmo tempo, desafia os Estados a equilibrar inovação tecnológica com a proteção dos direitos fundamentais, sobretudo no que diz respeito à privacidade, à vigilância e à soberania digital. É neste quadro que se tornam centrais as reflexões sobre os limites e potencialidades da atuação policial no combate ao cibercrime, o qual será dissecado no presente trabalho.

### 1.2. Enquadramento Teórico: Teorias Criminológicas no Ciberespaço

No âmbito da criminalidade informática, a ocorrência do ilícito não se circunscreve a um espaço físico delimitado nem obedece a fronteiras territoriais, manifestando-se sobretudo no domínio imaterial do ciberespaço. Segundo Paulo Nunes (2014), o ciberespaço "tornou-se um verdadeiro mediador das relações sociais e um motor do desenvolvimento económico dos países mais desenvolvidos. Assumindo-se como *global common*, o ciberespaço não tem fronteiras definidas." Para Antunes e Rodrigues (2018), "o ciberespaço consiste no espaço virtual que é criado através de comunicações e dos meios tecnológicos existentes", ou seja, é a infraestrutura que potencia as comunicações entre os utilizadores virtuais.

Desta forma, apesar das particularidades do cibercrime, várias teorias da criminologia clássica têm sido adaptadas com sucesso para compreender os comportamentos desviantes em ambiente digital. Uma das mais influentes é a Teoria da Atividade Rotineira, formulada por Cohen e Felson (1979), a qual sustenta que o crime ocorre quando convergem três elementos: um agressor motivado, uma vítima acessível e a ausência de um guardião eficaz. No ciberespaço, estes elementos são amplificados, designadamente, o anonimato facilita a motivação, a acessibilidade é global e a ausência de vigilância direta torna os ataques mais prováveis (Yar & Steinmetz, 2019).

Uma perspetiva teórica frequentemente mobilizada para compreender a escalada de comportamentos desviantes é a Teoria das Janelas Partidas, proposta por Wilson e Kelling (1982). Embora originalmente formulada no contexto urbano, esta abordagem foi posteriormente adaptada ao ambiente digital por diversos autores. No contexto do ciberespaço, defende-se que a tolerância a pequenas transgressões online, como comentários agressivos, discurso de ódio ou pirataria, pode favorecer a normalização de

comportamentos mais graves, criando um ecossistema permissivo à cibercriminalidade (García-Tejeda & Fondevila, 2023; Lanfear et al., 2020).

Do ponto de vista da aplicação da lei, estas teorias fornecem fundamentos teóricos para o reforço da vigilância digital e da monitorização preditiva. Contudo, também levantam preocupações éticas, sobretudo no que respeita à vigilância em massa e à proteção de dados pessoais (Haley, 2025). Assim, os paradigmas teóricos atuais procuram equilibrar segurança e direitos fundamentais, numa lógica de policiamento orientado por dados, mas sustentado por princípios democráticos.

### 1.3. Problematização da Cibercriminalidade e Hipóteses Conceptuais

A análise crítica da literatura recente permite sistematizar um conjunto de eixos conceptuais fundamentais para a compreensão aprofundada da cibercriminalidade e da resposta policial contemporânea. Estes eixos assentam em três dimensões interdependentes: a complexidade multidimensional do fenómeno, os limites das respostas tradicionais de policiamento e a necessidade imperativa de inovação integrada e colaborativa.

Em primeiro lugar, a cibercriminalidade manifesta-se como um fenómeno altamente dinâmico, transnacional e híbrido, que rompe com as categorias clássicas de tempo, espaço e jurisdição (Wall, 2007; Meulebroucke et al., 2025). A sofisticação crescente dos ataques, desde o *phishing* ao *ransomware*, da engenharia social ao acesso ilegítimo a infraestruturas críticas, revela uma criminalidade que não se limita à dimensão tecnológica, mas que se alimenta também da fragilidade cognitiva, da literacia digital deficiente e da própria estrutura descentralizada do ciberespaço. Assim, como defendem Yar e Steinmetz (2019), o cibercrime torna-se um reflexo das assimetrias estruturais do mundo digitalizado, exigindo uma leitura que vá além do paradigma técnico ou meramente repressivo.

Em segundo lugar, evidencia-se uma inadequação crescente dos modelos tradicionais de policiamento face aos desafios impostos pelo cibercrime. As investigações revelam que persiste um desfasamento entre a velocidade da inovação criminosa e a capacidade de atualização normativa, tecnológica e organizacional das forças de segurança (Hutchings & Holt, 2014). Por último, a eficácia da resposta policial depende da formação contínua dos seus agentes e da criação de ecossistemas de inteligência digital, pelo que se impõe a necessidade de uma transformação cultural, estruturada em torno de em três pilares estratégicos: qualificação tecnológica, formação e cooperação internacional.

Com base neste enquadramento, o presente trabalho propõe três hipóteses conceptuais orientadoras para o aprofundamento da análise:

H1 – Os desafios colocados pela cibercriminalidade resultam de uma assinalável assimetria estrutural entre os recursos e capacidades tecnológicas dos cibercriminosos e os recursos e formação à disposição dos polícias;

H2 – A superação deste hiato requer uma abordagem que transcenda o mero reforço tecnológico, exigindo uma reflexão profunda do modelo organizacional da PSP (vertente *ciber*) bem como uma revisão crítica do quadro normativo em vigor;

H3 – A cooperação internacional, enquanto fator decisivo para a gestão eficaz das fronteiras jurídicas no ciberespaço, permite mitigar tensões entre a soberania nacional e a necessidade de respostas conjuntas e coordenadas no combate à cibercriminalidade.

Estes contributos teóricos constituem, assim, a base estruturante para o próximo capítulo, a fim de estabelecer uma base conceptual sólida e fundamentar a construção de respostas mais eficazes, integradas e democraticamente legitimadas face à criminalidade informática do século XXI.

# 2. Perspetivas

No presente capítulo, propõe-se fazer uma análise crítica das principais relações, contradições e inconsistências identificadas no cruzamento entre o fenómeno da cibercriminalidade e a atuação policial. Com base nas hipóteses apresentadas no presente trabalho, examinam-se, por um lado, relações estruturantes entre policiamento, tecnologia e quadro legal, e por outro identificam-se contradições entre formação, inovação e legalidade. Por fim, são analisadas inconsistências digitais, no âmbito da cooperação internacional, da soberania nacional e dos desafios transfronteiriços. Esta abordagem permite, assim, identificar os desafios emergentes e as possibilidades de resposta do paradigma da segurança digital.

## 2.1. Relações estruturantes entre policiamento, tecnologia e quadro legal

### 2.1.1. A complexidade das tipologias de cibercrime e os limites legais da resposta policial

A crescente sofisticação das práticas criminosas no ciberespaço desafia as forças de segurança a atualizarem constantemente os seus métodos de prevenção e resposta. O cibercrime não é um fenómeno homogéneo; pelo contrário, caracteriza-se pela diversidade das suas formas, alvos, motivações e níveis de sofisticação tecnológica. Entre as principais tipologias destacam-se os crimes contra sistemas informáticos (como intrusão e sabotagem), crimes contra a integridade e disponibilidade dos dados (como o *ransomware*), e crimes com finalidade económica (como *phishing* e fraude online) (Wall, 2007; Europol, 2022). Esta multiplicidade tipológica impõe dificuldades operacionais à atuação policial, especialmente quando as infraestruturas digitais se estendem além das fronteiras nacionais.

Uma das limitações mais críticas reside na dificuldade de enquadramento jurídico de certos comportamentos. A transnacionalidade do cibercrime faz com que muitos crimes ocorram fora da jurisdição nacional, exigindo mecanismos de cooperação complexos e, por vezes, ineficazes. Como salienta Shukurov e Jafarov (2023), os compêndios legislativos nacionais ainda enfrentam lacunas significativas na tipificação de crimes informáticos emergentes, o que cria zonas cinzentas na sua persecução da ação penal.

Além disso, a velocidade com que surgem novas ameaças, como o uso de *deepfakes*, *malware* baseado em IA ou ataques coordenados por redes de *bots*, supera frequentemente a capacidade legislativa de acompanhar esses fenómenos. A Comissão

Europeia (2022) já alertava que "a resposta institucional permanece reativa e fragmentada, sobretudo nas áreas de tipificação penal e partilha de dados digitais entre países-membros". Esta fragmentação compromete não só a eficácia das investigações, mas também a harmonização de procedimentos, essencial para enfrentar crimes digitais com impacto transfronteiriço.

Em Portugal, em 1994, encontrava-se em vigor legislação destinada a regular os ilícitos relacionados com crimes informáticos, designadamente o Decreto-Lei n.º 252/94, de 20 de outubro, que "transpõe para a ordem jurídica interna a Directiva n.º 91/250/CEE, do Conselho, de 14 de maio, relativa ao regime de protecção jurídica dos programas de computador". Mais tarde, de forma a tipificar os crimes informáticos, o Código Penal, aprovado pelo Decreto-Lei n.º 48/95, de 15 de março, consagra um rol de crimes relacionados com o cibercrime, nomeadamente o crime de devassa através (…) da Internet, previsto no artigo 193.º; o crime de burla informática, constante no artigo 221.º ou o crime de branqueamento, nos termos do artigo 368.º-A. A Lei n.º 41/2004, de 18 de agosto, "transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas."

Somente a 15 de setembro de 2009, Portugal aprovou diversos diplomas de especial relevo para o combate à criminalidade informática, designadamente: a Convenção sobre o Cibercrime, adotada na cidade de Budapeste no dia 23 de novembro de 2001, através da publicação da Resolução da Assembleia da República n.º 88/2009, de forma a "intensificar a cooperação" internacional e a "prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade do cibercrime"; a Resolução da Assembleia da República n.º 91/2009, que aprova o "Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo a 28 de janeiro de 2003"; e, por último, foi publicada a Lei do Cibercrime, aprovada pela Lei n.º 109/2009, "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, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa" reunindo num único regime jurídico próprio o catálogo de crimes que "preveem a informática como um meio específico para atingir um bem jurídico geral". Porém, este quadro legal apresentado, tendo em consideração a constante evolução tecnológica, torna-se ineficaz e de certa forma, lento, visto que não consegue alcançar, com a mesma rapidez aquela evolução.

Como referem Yar e Steinmetz (2019), o cibercrime desafia as noções tradicionais de tempo, espaço e autoria criminal, exigindo das polícias não apenas competências técnicas, mas também um novo enquadramento epistemológico da criminalidade contemporânea. Isto obriga a um esforço integrado de atualização legislativa, sob pena de a atuação policial se revelar insuficiente face à velocidade de mutação dos crimes digitais.

### 2.1.2. Qualificação tecnológica e competências digitais das forças policiais

A capacidade de resposta das forças policiais face ao cibercrime encontra-se condicionada não apenas pela dotação tecnológica disponível, mas também pelo nível de literacia digital evidenciado pelos seus agentes. Segundo a United Nations Office on Drugs and Crime (UNODC) (2021), a ausência de formação especializada e de uma cultura institucional orientada para a tecnologia compromete significativamente a prontidão operacional das equipas de investigação criminal. Por sua vez, a literacia digital policial deve ser entendida não apenas como domínio técnico, mas como competência transversal, que abrange desde o conhecimento de infraestruturas digitais até à interpretação crítica de dados provenientes de dispositivos eletrónicos. Como defende Ganguli (2025), a literacia digital no contexto policial implica compreender o ciberespaço como um novo "território de patrulhamento", onde os sinais de risco e os padrões de comportamento exigem novos métodos de observação, prevenção e análise. Adicionalmente, os agentes enfrentam barreiras de tipo organizacional e institucional, como a resistência à mudança e a obsolescência tecnológica. Num mundo tecnológico em constante evolução e mutação, torna-se fulcral a existência de uma direta interoperabilidade entre bases de dados e a utilização, de forma criteriosa, da inteligência artificial (IA) nas investigações ao cibercrime. Conforme sublinham Lourenço et al. (2021), o cibercrime exige um reposicionamento epistemológico e estratégico da ação policial, que vá além da mera atualização pontual de ferramentas e que envolva também a formação ética, jurídica e prática dos seus profissionais. Neste sentido, a qualificação tecnológica deve incluir: i) formações regulares em tecnologias emergentes; ii) desenvolvimento de competências de investigação digital; iii) conhecimento dos regimes legais nacionais e internacionais aplicáveis; e iv) formação em gestão de crises digitais. Deste modo, só com uma abordagem holística será possível transformar as forças policiais, e em especial a PSP, num verdadeiro agente de cibersegurança pública.

Neste sentido, de forma a dar cumprimento às atribuições constantes na sua Lei Orgânica, a PSP, em 2017, através do Despacho n.º 6158/2017, de 13 de julho, efetivou a

criação de um serviço dedicado somente ao ambiente *ciber*, o Núcleo de Cibercriminalidade (NCIBER), estando inserido na Divisão de Investigação Criminal e Cooperação Internacional (DICCI), do Departamento de Investigação Criminal (DIC). Anos mais tarde, em 2024, com a publicação do Despacho n.º 1168/2024, de 31 de janeiro, e consequente restruturação das unidades orgânicas flexíveis da unidade Direção Nacional da PSP, o NCIBER passa a estar inserido na Divisão de Análise, Cibercriminalidade, Coordenação e Cooperação Internacional (DACCCI), do DIC. Esta divisão, tem como competência, entre outras, "representar a PSP em organizações e grupos de trabalho de âmbito nacional e internacional relativos à prevenção e investigação da cibercriminalidade, bem como aqueles destinados à partilha de informação e cooperação policial no âmbito da cibercriminalidade". Concluímos assim, que atualmente a PSP tem, formalmente, um Núcleo criado, já com alguma maturidade, a trabalhar a área ciber, de forma a dar cumprimento à constante evolução tecnológica e consequentemente à criminalidade informática associada.

## 2.2. Contradições entre formação, inovação e legalidade

### 2.2.1. Formação policial e literacia digital: a formação como eixo estratégico

A eficácia da atuação policial perante a cibercriminalidade depende não apenas da existência de legislação adequada ou de recursos tecnológicos avançados, mas também da formação contínua dos seus agentes. A natureza sofisticada e em constante mutação dos crimes digitais exige competências técnicas específicas, bem como uma sólida literacia digital entre os profissionais da segurança pública (Ogg et al., 2024).

Formação especializada em cibersegurança e investigação digital revela-se fundamental. Segundo Harkin & Whelan (2021), a ausência de programas formativos regulares e estruturados é apontada como uma das principais fragilidades das forças policiais, originando lacunas tanto ao nível da resposta operacional imediata como na gestão estratégica de casos complexos. De acordo com o relatório do Conselho da Europa e INTERPOL, são indispensáveis estratégias de formação em camadas, que combinem treino técnico, simulações práticas e atualização constante, para garantir uma resposta eficaz às crescentes ameaças digitais (Conselho da Europa & Interpol, 2022). Exemplos de práticas recomendadas incluem o estabelecimento de sistemas de aprendizagem contínua, cursos modulares adaptados às necessidades locais e partilha de conhecimento entre as forças e os serviços de segurança e os países membros da UE, como promovido pelo European Cybercrime Training and Education Group (ECTEG).

Em Portugal, o protocolo celebrado entre a PSP e a entidade gestora do domínio .PT reforçam o compromisso de promover a formação avançada dos agentes em técnicas e ferramentas de cibersegurança, criando sinergias entre investigação operacional e inovação tecnológica (.PT, 2024). Investir na formação e na literacia digital dos agentes policiais é, portanto, eixo estratégico para o sucesso das investigações e para a resiliência das instituições de segurança face às novas ameaças digitais. De acordo com relatórios internacionais, somente com estratégias coordenadas e investimento contínuo em capital humano permitirão que as forças policiais estejam preparadas para responder com eficiência e competência aos desafios do cibercrime (Council of Europe & INTERPOL, 2022). Consultados os planos curriculares das várias unidades curriculares que compõem o Curso de Formação de Oficiais de Polícia (CFOP), ministrado no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), e os Cursos de Formação de Chefes (CFC) e de Agentes (CFA), ministrados na Escola Prática de Polícia (EPP), claramente chegou-se à conclusão que a formação em cibercrime é insuficiente e encontra-se ainda pouco desenvolvida, o que irá colocar em causa o futuro próximo, em termos de prevenção, repressão e investigação desta nova forma de criminalidade, bem como todo o seu novo paradigma de ciberpoliciamento. Segundo Afonso (2024), a PSP, no final do ano de 2024, através do NCIBER, desenvolveu um curso de formação de cibercriminalidade para *first responders* (eFIRST) em colaboração com o ECTEG (European Cybercrime Training and Education Group). Foi composto por “peritos e especialistas de cibercriminalidade e cibersegurança, de várias Polícias europeias” e teve como objetivo claro a implementação nas unidades curriculares dos “cursos de formação de polícias”, ou seja, no CFOP, CFC e CFA, de matérias especificas de cibercrime, o que, na realidade, não se materializou na prática.

Por outro lado, a literacia digital não pode ser entendida apenas como domínio técnico. Implica também capacidades analíticas, éticas e legais, capazes de sustentar uma atuação proporcional e juridicamente segura em ambientes digitais complexos (Santos et al., 2016). Como defendem Carvalho et al. (2020), é essencial desenvolver uma doutrina comum de atuação cibernética, assente em protocolos bem definidos, interoperabilidade técnica e partilha de boas práticas. Além desta formação interna, a cooperação com universidades, centros de investigação, agências europeias (como a Europol) e com o setor privado, são cruciais e terão de ser, obrigatoriamente, o presente e o futuro no combate a esta criminalidade informática. Enquanto plataforma europeia de cooperação, o EMPACT (European Multidisciplinary Platform Against Criminal Threats) tem desempenhado um

papel relevante na disponibilização de formação especializada e na partilha de inteligência entre os Estados-Membros, promovendo uma abordagem multilateral ao problema da cibercriminalidade (CEPOL, 2024).

No entanto, para além das formações pontuais, impõe-se um modelo de desenvolvimento contínuo e transversal na PSP, de forma a promover as competências digitais ao longo de toda a carreira de todos os seus polícias. Porém, para ser concretizável será necessário a existência de um planeamento estratégico e de uma avaliação rigorosa das matérias lecionadas nos dois estabelecimentos de ensino policial, o ISCPSI e a EPP.

### 2.2.2. Lacunas legais e atualização legislativa

A rápida evolução tecnológica tem colocado o direito penal e processual penal perante um dilema estrutural: como responder eficazmente a novas formas de criminalidade digital sem comprometer garantias fundamentais? Esta tensão entre inovação criminógena e rigidez normativa tornou-se um dos principais entraves à atuação policial no domínio da cibercriminalidade (Rahka, 2025). Em muitos ordenamentos jurídicos, os tipos legais de crime não contemplam condutas digitais emergentes, como ataques de *ransomware*, manipulação algorítmica, engenharia social ou apropriação de identidades digitais através de *deepfakes*. Mesmo nos países com legislação específica, como Portugal, o enquadramento legal é frequentemente genérico, exigindo interpretações extensivas que nem sempre resistem ao crivo constitucional (Dias et al., 2025). Esta insuficiência normativa compromete a previsibilidade jurídica e dificulta a responsabilização penal dos cibercriminosos, sobretudo quando se recorre a redes descentralizadas ou identidades encriptadas. Além disso, as leis processuais mostram-se desadequadas para lidar com provas digitais voláteis e transnacionais. Contudo, em muitos sistemas jurídicos, subsiste uma ausência de regras claras sobre admissibilidade de provas recolhidas por meios digitais, em especial quando obtidas com recurso a colaboração internacional ou através de plataformas privadas (Raburu & Dinga, 2020).

Em Portugal, a Lei do Cibercrime (Lei n.º 109/2009) representa um passo importante na tipificação de crimes informáticos, alinhando-se com os princípios da Convenção de Budapeste. Contudo, passados mais de 15 anos desde a sua aprovação, surgem críticas quanto à sua atualização e capacidade de resposta. Novas ameaças digitais, como o *phishing* automatizado por IA, a criminalidade em ambientes imersivos (metaverso) e os ataques a infraestruturas críticas via Internet das Coisas (IoT), permanecem insuficientemente regulados (Achuthan et al., 2025). Stol et al. (2025),

destacam que a modernização legislativa só será eficaz se for acompanhada com formação dos polícias e com um investimento estratégico nas forças de segurança.

A eficácia da atuação policial perante a cibercriminalidade não depende exclusivamente da existência de enquadramentos legislativos adequados ou de recursos tecnológicos avançados, mas sobretudo da qualificação e da formação contínua dos seus agentes. Em Portugal, a análise dos planos curriculares do ISCPSI e da EPP evidencia lacunas significativas na formação em cibercrime, o que compromete a prevenção, a repressão e a investigação desta forma de criminalidade. Paralelamente, a rápida evolução tecnológica desafia a atualização normativa, tornando obsoletos vários dispositivos legais, nomeadamente os previstos na Lei do Cibercrime. A ausência de um quadro legal dinâmico e a carência de investimento sistemático em capital humano e em cooperação internacional limitam a capacidade da PSP em responder, de forma eficaz, às novas ameaças digitais.

## 2.3. Inconsistências digitais: cooperação, soberania e desafios transfronteiriços

### 2.3.1. A cooperação internacional e os constrangimentos inerentes à soberania digital

A natureza transnacional da cibercriminalidade coloca um dos maiores desafios às forças policiais contemporâneas: a gestão das fronteiras jurídicas no ciberespaço. Ao contrário da criminalidade tradicional, cujas manifestações tendem a restringir-se a territórios delimitados, os crimes digitais frequentemente envolvem autores, vítimas, servidores e conteúdos localizados em múltiplas jurisdições, dispersos por diferentes países, o que torna as investigações complexas, lentas e, muitas vezes, ineficazes (Ajayi, 2016; Conselho da Europa, 2023).

Embora o ciberespaço seja percebido como um território sem fronteiras físicas, os sistemas jurídicos mantêm-se profundamente ancorados na soberania nacional. Assim, a aplicação da lei torna-se difícil quando os dados ou os cibercriminosos estão fora do território nacional. Esta fragmentação é aproveitada por redes criminosas para operar em países com leis menos rígidas ou com ausência de acordos de cooperação legal (Carvalho, 2019). Face a este carácter transfronteiriço, é imperiosa a necessidade de novas formas de cooperação policial promovidas por organismos como a INTERPOL, Europol e o UNODC, que facilitam o intercâmbio de informações, sobretudo a Estados com menor capacidade tecnológica (INTERPOL, 2025; UNODC, 2021). Apesar do protagonismo destas entidades, permanecem obstáculos relevantes: a desigualdade tecnológica entre países, a fragmentação dos enquadramentos legais e a resistência de certas jurisdições à

partilha de dados sensíveis, o que compromete frequentemente a eficácia das ações conjuntas (Conselho da Europa, 2025). De forma particular, conforme já foi aqui aludido, a ausência de normativos internacionais harmonizados dificulta a criminalização dos autores deste tipo de crimes, criando, em termos legais, verdadeiras "zonas cinzentas" (UNODC, 2021).

A título ilustrativo, a Convenção de Budapeste sobre o Cibercrime, promovida pelo Conselho da Europa e subscrita por mais de 65 países, estabelece um conjunto de normas mínimas para a investigação e cooperação internacional nesta matéria. Contudo, importantes potências digitais como a China, a Rússia e a Índia recusaram a sua ratificação, alegando ingerência na sua soberania digital e contestando a hegemonia normativa ocidental (Conselho da Europa, 2024). Este cenário fragmentado dificulta a construção de uma arquitetura global de resposta ao cibercrime, uma vez que é inconcebível a implementação de uma legislação global, face à soberania de cada país e à constante e rápida evolução da cibercriminalidade.

No contexto da União Europeia, programas como o European Cybercrime Centre (EC3), da Europol, fortalecem a articulação operacional, enquanto plataformas da INTERPOL, como a rede I-24/7, sustentam canais privilegiados de cooperação, dos quais Portugal é membro ativo (INTERPOL, 2025). Em 2023, a Europol participou em mais de 400 ações de combate ao cibercrime com impacto direto em países da União Europeia, incluindo Portugal (Europol, 2024). Apesar disso, limitações persistem, sobretudo na recolha transnacional da prova digital e na articulação com empresas tecnológicas globais. Veja-se que várias plataformas sediadas fora da União Europeia, em particular as norte-americanas, tendem a condicionar ou a rejeitar o acesso aos dados com fundamento em legislações nacionais de proteção de privacidade, como o CLOUD Act (EUA) ou o GDPR (UE), evidenciando a tensão constante entre necessidades investigativas e direitos digitais (Mignon, 2021; Mroz, 2025). Tal dilema traduz-se num paradoxo entre segurança digital e soberania informacional. Por um lado, forças policiais dependem de acesso célere a dados transfronteiriços e, por outro, Estados e empresas tecnológicas impõem restrições fundadas na proteção da privacidade e autonomia digital (Kaya & Shahid, 2025). Hardzinski (2016) caracteriza a internet global como um autêntico "campo de batalha geopolítico", em que infraestruturas digitais funcionam simultaneamente como instrumentos de regulação, poder e resistência.

Um dos caminhos mais promissores reside no desenvolvimento de mecanismos multilaterais de confiança tecnológica, capazes de conciliar os imperativos de segurança e

soberania digital. No plano internacional, a Organização das Nações Unidas (ONU) promove fóruns de governação digital e cooperação técnica, enquanto a UE aposta em projetos como a cloud europeia GAIA-X, visando garantir autonomia estratégica e padrões de interoperabilidade consentâneos com a proteção de dados (Musiani, 2025). Portugal, firmando-se como subscritor da Convenção de Budapeste e participante ativo em fóruns europeus e globais, está bem posicionado para contribuir na arquitetura de soluções inovadoras que equilibrem a justiça digital e a soberania informacional (Sarmento e Castro, 2022).

### 2.3.2. Mecanismos transfronteiriços: desafios da jurisdição digital

Efetivamente, a cooperação internacional tem avançado através de programas e projetos que promovem o intercâmbio de informação em tempo real, operações conjuntas e formação técnica entre países membros. Contudo, os desafios permanecem relevantes, como é o caso da obtenção de provas digitais transfronteiriças. Frequentemente, esta preservação de prova é travada por procedimentos demorados, como os pedidos de cooperação judiciária internacional (MLA – mutual legal assistance). Para agilizar este processo, a União Europeia adotou o regulamento e-evidence, que pretende permitir às autoridades nacionais aceder diretamente a dados armazenados em servidores de empresas tecnológicas, mesmo que localizados noutro país membro (Stefan & Fuster, 2018). No entanto, esta proposta tem suscitado críticas por potenciais conflitos de soberania nacional (eventual choque com a legislação dos Estados Membros), de violação da privacidade, de garantias processuais e do Regulamento Geral de Proteção de Dados (RGPD).

Por outro lado, países como os EUA impuseram acordos bilaterais com base no CLOUD Act, que facilita o acesso a dados sob jurisdição americana. Tais acordos levantam questões sensíveis quanto à reciprocidade, proteção de dados e ingerência legal, o que reforça a necessidade de soluções equilibradas no plano internacional. Porém, a falta de harmonização legislativa global é um entrave para a existência de cooperação. Note-se que países como a China e a Rússia não participam em convenções internacionais amplamente aceites, o que dificulta o rastreio e a responsabilização de cibercriminosos nesses territórios. Esta ausência de consenso global é apontada como um fator de proliferação de atividades ilícitas, especialmente no que se refere a ataques de *ransomware* (Fidler, 2025).

No plano nacional, Portugal tem reforçado a sua atuação através de colaborações com o Eurojust e a Rede Judiciária Europeia, promovendo ações conjuntas e formação

técnica. A única Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, e ainda sem uma atualização para os próximos anos, reforça o "compromisso de aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente".

Em síntese, as perspetivas analisadas neste capítulo revelam a existência de uma série de tensões que comprometem a eficácia da resposta policial à cibercriminalidade. Verifica-se que a expansão transnacional da cibercriminalidade desafia os princípios clássicos da soberania e da jurisdição penal, evidenciando as limitações dos enquadramentos jurídicos nacionais perante um ciberespaço "desterritorializado". A fragmentação normativa e a desigualdade tecnológica entre Estados dificultam a cooperação internacional e favorecem a proliferação de "zonas cinzentas". Os instrumentos como a Convenção de Budapeste e mecanismos internacionais, como a INTERPOL e a Europol, constituem tentativas relevantes de harmonização, embora persistam resistências fundadas na defesa da soberania digital. No contexto europeu, o regulamento e-evidence surge como resposta à morosidade dos pedidos de cooperação judiciária. Paralelamente, acordos como o CLOUD Act norte-americano ilustram a assimetria regulatória e os riscos de ingerência jurídica. Portugal, enquanto signatário ativo e participante em estruturas europeias, procura equilibrar a segurança digital, a proteção dos direitos fundamentais e a autonomia soberana num ecossistema global interdependente. Subsequentemente, abordar-se-ão em maior detalhe estas implicações, com vista a propor uma reflexão final sobre as implicações teóricas e práticas do trabalho desenvolvido.

## Discussão

O combate à cibercriminalidade representa um dos maiores desafios contemporâneos para as forças de segurança, exigindo da PSP uma adaptação constante aos novos contextos tecnológicos e operacionais. A crescente sofisticação das ameaças digitais, aliada à sua natureza transnacional, impõe uma resposta integrada que combine inovação tecnológica, formação especializada e cooperação internacional. A PSP tem procurado reforçar as suas capacidades através da criação o NCIBER, contudo, persistem constrangimentos significativos, sendo necessário compreender os desafios e as respostas da PSP neste domínio. Um dos principais desafios reside na escassez de formação, quer seja inicial, contínua ou de especialização, pelo que se propõe: i) formação inicial e

contínua inserida no CFOP, CFA e CFC, respetivamente; ii) formações regulares em tecnologias emergentes para o efetivo policial que labore no âmbito *ciber*; iii) aperfeiçoamento das competências em investigação digital; iv) conhecimento aprofundado dos regimes jurídicos nacionais e internacionais; e v) formação dos polícias em gestão de crises digitais. Assim, a PSP, enquanto ator estratégico de cibersegurança e garante da resiliência digital no espaço público, deverá integrar esta abordagem na sua esfera estrutural, de modo a consolidar a sua capacidade de resposta integrada a incidentes cibernéticos. Outro obstáculo prende-se com a necessidade de "dar o salto" dos métodos tradicionais de policiamento (Johnson et al., 2020), para um policiamento preditivo, de modo a dar resposta à evolução tecnológica e às novas abordagens de segurança pública digital. Caso a PSP não se adapte a esta evolução de novos modelos de policiamento, irá ficar, seguramente, com uma limitação na capacidade de resposta proativa e com uma abordagem predominantemente reativa no combate ao cibercrime, o que não é desejável numa instituição secular e que se pretende nivelada com os progressos tecnológicos.

Além disso, a complexidade e diversidade do cibercrime impõem desafios significativos à atuação policial, sobretudo quando as infraestruturas digitais ultrapassam as fronteiras estatais. Uma limitação central reside na dificuldade de enquadramento jurídico de condutas transnacionais, que exigem a utilização de mecanismos de cooperação internacionais. De igual modo, persistem lacunas legais na tipificação de novas formas de criminalidade informática, criando zonas cinzentas na qual os cibercriminosos operam com total impunidade (Amoo et al., 2024). Ademais, a rápida emergência de ameaças como *deepfakes*, *malware* baseado em IA e ataques de *bots* supera claramente a capacidade de adaptação legislativa, comprometendo a eficácia e celeridade da resposta policial. No contexto atual, verifica-se que existe um enorme desfasamento entre a evolução tecnológica e a atualização dos quadros legais e normativos. Contudo, conforme argumenta Neiva (2025), a aplicação sistemática de tecnologias como IA, análise preditiva e *big data* nas polícias portuguesas ainda é, em parte, fragmentada e enfrenta constrangimentos de regulação, de interoperabilidade e de recursos humanos, estando em evolução para uma adoção mais estruturada.

Em síntese, o combate à cibercriminalidade impõe à PSP uma adaptação a novos modelos de policiamento, designadamente o preditivo (*predictiv policing*) bem como uma interligação entre formação e a realidade operacional digital. Sem esta evolução integrada, a PSP corre o risco de manter uma abordagem predominantemente reativa, comprometendo a sua capacidade de assegurar a resiliência digital e a proteção do espaço

cibernético da sua responsabilidade.

## Conclusão

A análise desenvolvida ao longo deste trabalho permitiu compreender, com maior profundidade, os impactos multifacetados da cibercriminalidade sobre a atuação policial contemporânea. Confirmou-se que os desafios colocados por este fenómeno não se esgotam na sua vertente técnica ou operacional, mas implicam transformações mais amplas ao nível institucional, jurídico e epistemológico.

Relativamente às hipóteses conceptuais formuladas, o presente estudo atestou que (H1) existe um assinalável desfasamento entre os recursos tecnológicos ao serviço dos cibercriminos e aqueles que estão à disposição dos polícias, sendo necessário qualificar tecnologicamente todo o efetivo, reforçando com meios humanos o NCIBER, como ponto central de análise, prevenção, repressão e investigação da cibercriminalidade. De igual modo, (H2) a constante evolução tecnológica requer igualmente uma atualização constante do quadro legislativo nacional, de forma a eliminar lacunas legais na tipificação de novas ameaças digitais, como o *phishing* automatizado por IA, a criminalidade em ambientes imersivos (metaverso) e os ataques a infraestruturas críticas via Internet das Coisas (IoT). No plano internacional (H3) "as ciberameaças e a cibercriminalidade em concreto, estão cada vez mais organizadas e transvazam fronteiras geográficas, de soberania política, de origem social e económica e tecnológicas" (Elias, 2019), pelo que é essencial a existência de novas formas de cooperação policial promovidas por organismos como a INTERPOL, Europol e o UNODC, de forma a facilitar o intercâmbio de informações, sobretudo em Estados com menor capacidade tecnológica. A Convenção de Budapeste, a rede I-24/7 da INTERPOL e o European Cybercrime Centre (EC3) demonstram que a cooperação multilateral permite mitigar limitações decorrentes da soberania nacional. Contudo, disparidades tecnológicas, resistência normativa e a ausência de adesão de alguns países criam obstáculos, reforçando a necessidade de mecanismos harmonizados e protocolos de confiança internacional. Pelo exposto, verifica-se que as hipóteses identificadas foram amplamente confirmadas.

Do ponto de vista teórico, o estudo contribuiu para o alargamento do campo de análise das ciências policiais na área *ciber*, demonstrando que a cibercriminalidade exige novas abordagens interdisciplinares. A articulação entre teorias criminológicas clássicas, como a Teoria da Atividade Rotineira ou a Teoria das Janelas Partidas, e as

particularidades do ciberespaço revelaram-se úteis para interpretar dinâmicas criminais emergentes, embora insuficientes se não forem acompanhadas por um enquadramento legislativo constante e por uma atualização tecnológicas das polícias. O conceito de "policiamento digital competente" surge, neste contexto, como um novo paradigma, que exige não apenas conhecimento técnico, mas também consciência crítica sobre as implicações da vigilância, da privacidade e da soberania informacional.

Do ponto de vista prático, os resultados obtidos permitem formular um conjunto de recomendações estratégicas. Em primeiro lugar, face à insuficiente formação no domínio da cibercriminalidade, impõe-se um modelo de desenvolvimento contínuo e transversal na PSP, de forma a promover as competências digitais ao longo de toda a carreira de todos os seus polícias. Para a sua concretização será necessário a existência de um planeamento estratégico e dotar os planos curriculares do CFOP, o CFC e o CFA com módulos curriculares dedicados ao estudo da criminalidade informática. De igual forma, o curso de formação de cibercriminalidade para *first responders* (eFIRST) deve ser potenciado para os polícias que atuam em contextos de cibersegurança. É ainda essencial desenvolver uma doutrina comum de atuação cibernética, assente em protocolos bem definidos, interoperabilidade técnica e partilha de boas práticas. Além da formação interna, propõem-se, em consonância com a argumentação de Carvalho et al. (2020), que a cooperação com universidades, centros de investigação, agências europeias e com o setor privado, sejam vistas como cruciais e obrigatórias no presente e no futuro, para o combate a esta criminalidade informática. Em segundo lugar, tendo em conta a rápida evolução tecnológica, torna-se necessário atualizar os quadros legais e processuais de forma mais ágil e célere, integrando, se viável, mecanismos que envolvam decisores políticos, especialistas em tecnologia e a sociedade civil, de forma a criar um enquadramento legal e evitar a existência de um vazio legislativo, face às novas e atuais ameaças digitais. Em terceiro lugar, a cooperação internacional deve ser fortalecida por via de mecanismos multilaterais mais eficazes e inclusivos, capazes de ultrapassar as atuais tensões entre soberania nacional e partilha de dados transfronteiriços. O combate à cibercriminalidade não pode ser encarado como um domínio especializado e isolado, mas sim como uma dimensão transversal da segurança pública no século XXI. À luz deste facto, verifica-se a participação ativa de Portugal em redes europeias de cibersegurança, bem como o seu contributo em iniciativas como o GAIA-X, que podem posicionar o país como um ator relevante na construção de um espaço digital mais seguro e justo.

O trabalho aqui apresentado permite, assim, concluir que a eficácia da atuação

policial, perante a cibercriminalidade, depende de uma abordagem integrada, conjugada com a qualificação tecnológica, formação policial e atualização normativa face aos novos paradigmas tecnológicos, promovendo um modelo de policiamento adaptado às complexidades do ciberespaço (*predictiv policing*). Trata-se, em última análise, de garantir que os princípios do Estado de Direito não se perdem nas novas fronteiras digitais, mas antes se reforçam como garantias fundamentais da justiça e da segurança coletiva.

Conclui-se, afirmando, que o futuro da cibercriminalidade representa um enorme desafio, exigindo da PSP uma alteração de paradigma relativo ao ciberpoliciamento, sob pena de comprometer, de forma irreversível, a sua capacidade de prevenção, reação e controlo das novas ameaças da criminalidade digital.

# Referências


Achuthan, K., Ramanathan, S., & Raman, R. (2025). Securing the metaverse: Machine learning–based perspectives on risk, trust, and governance. *International Journal of Information Management Data Insights*, *5*(2), 100356. https://doi.org/10.1016/j.jjimei.2025.100356

Afonso, P. (2024), *Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS*, ISCPSI.

Ajayi, E. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems, 6*(1), 1-12. https://doi.org/10.5897/JIIS2015.0089

Alves, A. (2025). *O aumento da criminalidade deve-se aos cibercrimes e não aos imigrantes, diz director da PJ*. Público. https://www.publico.pt/2025/02/26/sociedade/noticia/aumento-criminalidade-devese-cibercrimes-nao-imigrantes-director-pj-2123968

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy and Development*, *8*(10), 1-20. https://doi.org/10.24294/jipd.v8i10.6007

Amoo, O., Atadoga, A., Abrahams, T., Farayola, O., Osasona, F. & Ayinla, B. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews, 21*(02), 205-217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança - A internet, os aspetos legais e a análise digital forense.* FCA.

Aviso n.º 8826/2019. (2019). *Estrutura curricular e o plano de estudos do ciclo de estudos de mestrado integrado em Ciências Policiais do ISCPSI*. Diário da República n.º 98/2019, Série II de 2019-05-02, páginas 15848 – 15850. http://www.iscpsi.pt/Cursos/cfop/PlanoCurricular/Paginas/default.aspx

Carvalho, A. (2019). Ciberespaço e os novos desafios à soberania e à segurança dos Estados. IDN V Seminário Jovem. *IDN Cadernos*, 36, 219-235.

Carvalho, J., Rocha, Á., Abreu, A. & Victor, A. (2020). Portuguese Concerns and Experience of Specific Cybercrimes: A Benchmarking with European Citizens. In *Developments and Advances in Defense and Security - Proceedings of MICRADS*

*2019.* https://researchportal.ulisboa.pt/en/publications/portuguese-concerns-and-experience-of-specific-cybercrimes-a-benc

CEPOL (2024). *EMPACT 2024 Results*. https://www.consilium.europa.eu/media/3qdixbn0/2025_2020_empact-factsheets-2024_onepage_04_print.pdf

Centro Nacional de Cibersegurança (2025). *Estratégia Nacional*. https://www.cncs.gov.pt/pt/estrategia-nacional/

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Comissão Europeia (2022). *Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2022:49:FIN

Conselho da Europa & Interpol (2022). Guide for developing law enforcement training strategies on cybercrime and electronic evidence. https://rm.coe.int/guide-for-developing-training-strategies-final/1680a62c72

Conselho da Europa (2023). *C-PROC delegates attend the Annual Conference of the European Cybercrime Centre (EC3).* https://www.coe.int/en/web/cybercrime/-/c-proc-delegates-attend-the-annual-conference-of-the-european-cybercrime-centre-ec3-

Conselho da Europa (2024). *The "Budapest" Convention on Cybercrime and the draft United Nations treaty: links.* https://www.coe.int/en/web/cybercrime/-/the-budapest-convention-on-cybercrime-and-the-draft-united-nations-treaty-links

Conselho da Europa (2025). *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols.* https://www.coe.int/en/web/cybercrime/the-budapest-convention

Cucoreanu, C. (2024). Efficiency of Police Cooperation in Criminal Investigations. *European Journal of Law and Public Administration*, *11*(1), 24–38. https://doi.org/10.18662/eljpa/11.1/218

Decreto-Lei n.º 252/94 (1994). *Transpõe para a ordem jurídica interna a Directiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de protecção jurídica dos programas de computador.* Diário da República n.º 243/1994, Série I de 1994-10-20, páginas 6374 – 6376. https://files.diariodarepublica.pt/1s/1994/10/243a00/63746376.pdf

Decreto-Lei n.º 48/95. (1995). *Código Penal.* Diário da República n.º 63/1995, Série I de 1995-03-15, páginas 1350 – 1416. https://files.diariodarepublica.pt/1s/1995/03/063a00/13501416.pdf

Despacho n.º 6158/2017. (2017). *Definidas as unidades orgânicas flexíveis da Direção Nacional da Polícia de Segurança Pública (PSP), bem como as correspondentes competências.* Diário da República n.º 134/2017, Série II de 2017-07-13, páginas 14526 – 14529. https://diariodarepublica.pt/dr/detalhe/despacho/6158-2017-107677747

Despacho 28/GDN/2022. (2022). *Aprova o Regulamento de Frequência e Avaliação do Curso de Formação de Chefes da Polícia de Segurança Pública*. Ordem de Serviço Nacional da Direção Nacional, n.º 28, I Parte de 2022-11-24.

Despacho n.º 1168/2024. (2024). *Define as unidades orgânicas flexíveis da unidade Direção Nacional da PSP*. Diário da República n.º 22/2024, Série II de 2024-01-31, páginas 45 – 83. https://diariodarepublica.pt/dr/detalhe/despacho/1168-2024-839796305

Despacho (extrato) n.º 12448/2024. (2024). *Aprova o Regulamento de Frequência e Avaliação do Curso de Formação de Agentes da Polícia de Segurança Pública.* Diário da República n.º 204/2024, Série II de 2024-10-21. https://diariodarepublica.pt/dr/detalhe/despacho-extrato/12448-2024-891537146

Dias, S., Camilo, I. & Dias, A. (2025). *The Rise of Cybercrime: Challenges and Precautions in the Digital Age.* https://www.caiadoguerreiro.com/en/the-rise-of-cybercrime-challenges-and-precautions-in-the-digital-age/

Elias, L. (2018). *Ciências policiais e segurança interna, desafios e prospetiva.*ISCPSI.

Elias, L. (2019). Ciberameaças e (In)segurança. *Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa*. https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_7.pdf

European Union Agency for Cybersecurity (2024). *2024 Report on the state of cybersecurity in the Union*. https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Europol (2022). *Europol Programming Document 2023 – 2025.* https://secure.ipex.eu/IPEXL-WEB/download/file/8a8629a8859f33e70185a0a6367c0015/Europol_Programming_Document_2023_2025.pdf

Europol (2024). *Uncovering the Ecosystem of Intellectual Property Crime. A focus on enablers and impact*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Uncovering_the_ecosystem_of_IP_Crime_report/2024_Uncovering_the_ecosystem_of_IP_Crime_FullR_en.pdf

Europol (2025). *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Federal Bureau of Investigation (2025). *Internet Crime Report 2024*. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Fidler, M. (2025). Fragmentation of International Cybercrime Law. *Utah Law Review*, 3, 737-804. https://dc.law.utah.edu/cgi/viewcontent.cgi?article=1413&context=ulr

Ganguli, P. (2025). Digital Policing: Using Social Media Surveillance to Tackle Cybercrime. *SSRN*. http://dx.doi.org/10.2139/ssrn.5124657

García-Tejeda, E., & Fondevila, G. (2023). Policing Social Disorder and Broken Windows Theory: Spatial Evidence from the "Franeleros" Experience. *ISPRS International Journal of Geo-Information*, *12*(11), 449. https://doi.org/10.3390/ijgi12110449

Haley, P. (2025). The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. *Sensors, 25*(10), 3160. https://doi.org/10.3390/s25103160

Hardzinski, B. (2016). *The Complicated Geopolitical Issues Surrounding Who Controls The Internet.* https://www.kgou.org/world/2016-02-05/the-complicated-geopolitical-issues-surrounding-who-controls-the-internet

Harkin, D., & Whelan, C. (2021). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, *24*(1), 66-76. https://doi.org/10.1177/14613557211036565 (Original work published 2022)

Hutchings, A. & Holt, T. (2014). A Crime Script Analysis of the Online Stolen Data Market. *The British Journal of Criminology*, 55(3), 596–614. https://doi.org/10.1093/bjc/azu106

Interpol (2024). *Annual Report 2023.* https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf

Interpol (2025). *How INTERPOL supports Portugal to tackle international crime.* https://www.interpol.int/en/Who-we-are/Member-countries/Europe/PORTUGAL

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet Crimes.* Willan.

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law*, *84*(5), 427-450. https://doi.org/10.1177/0022018320952559

Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(2), 219–233. https://doi.org/10.61838/kman.isslp.4.2.20

Klymenko, O., Gutsaliuk, M., & Savchenko, A. (2020). Combating Cybercrime as a Prerequisite for the Development of Digital Society. *e-Journal of International Relations, 11*(1), 18-29. https://doi.org/10.26619/1647-7251.11.1.2

Lanfear, C. C., Matsueda, R. L., & Beach, L. R. (2020). Broken Windows, Informal Social Control, and Crime: Assessing Causality in Empirical Studies. *Annual Review of Criminology*, *3*(1), 97–120. https://doi.org/10.1146/annurev-criminol-011419-041541

Lei n.º 109/2009 da Assembleia da República. Diário da República n.º 179/2009, Série I de 2009-09-15, páginas 6319 – 6325. https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693

Lesmana, D., Afifuddin, M. & Adriyanto, A. (2023). Challenges and Cybersecurity Threats in Digital Economic Transformation. *International Journal Of Humanities Education and Social Sciences (IJHESS)*, *2*(6). https://doi.org/10.55227/ijhess.v2i6.515

Lourenço, R., Frade, C., Mendes, J., Almeida, L. Melo, M., Cerqueira, P. & Mota, S. (2021*). Cibersegurança em Portugal: Políticas Públicas*. Faculdade de Economia da Universidade de Coimbra e CNCS. https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/observatorio_ciberseg_relatorio_politicas_publicas.pdf

Marques, G., & Martins, L. (2006). *Direito da Informática.* Coimbra: Almedina.

Meulebroucke, L., Emplit, K. & Mauquoy, M. (2025). The digitalisation of the police. . In *Legal and Ethical Issues in Digital Policing: Policing in the Digital Society Network Yearbook 2025* (pp. 59-81). Boom.

Mignon, E. (2021). *The CLOUD Act: Unveiling European Powerlessness*. https://geopolitique.eu/articles/the-cloud-act-unveiling-european-powerlessness/

Ministério da Administração Interna (2025). *Relatório Anual de Segurança Interna RASI 2024.* https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDExNwYAs4WfKQUAAAA%3d

Mroz, I. (2025). *Understanding the U.S. Cloud Act: Impact on Compliance, Agreement, and Data Protection*. https://www.archtis.com/understanding-the-us-cloud-act/

Musiani, F. (2025). *Gaia-X: the bid for a sovereign European cloud*. https://www.polytechnique-insights.com/en/columns/digital/gaia-x-the-bid-for-a-sovereign-european-cloud/

Neiva, L. (2025). *Big Data na polícia: inovação ou vigilância?* https://www.communitas.pt/ideia/big-data-na-policia-inovacao-ou-vigilancia/

Nunes, P. V. (2014). Ciberespaço, ciberviolência e o uso organizado da força. *Metamorfoses da violência*, pp. 146-147.

Ogg, J., McShane, L. & Patrick, E. (2024). *Duty To Data Upskilling police and operational agencies.* https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2024/nov/upskilling-police-and-operational-agencies.pdf

Raburu, G. & Dinga, L. (2020). Legal Issues in Computer Forensics and Digital Evidence Admissibility. *International Journal of Computer Science and Mobile Computing, 9*(7), 86-89. https://www.researchgate.net/publication/344695331_Legal_Issues_in_Computer_Forensics_and_Digital_Evidence_Admissibility

Rakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican law review*, *16*(2), 23-54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho. (2023). *Ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais – e-evidence.* Jornal Oficial da União Europeia, L 191/118, 2023-07-28. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32023R1543

Resolução da Assembleia da República n.º 88/2009. (2009). *Aprova a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001*. Diário da

República n.º 179/2009, Série I de 2009-09-15, páginas 6354 – 6378. https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/88-2009-489698

Resolução da Assembleia da República n.º 91/2009. (2009). *Aprova o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adoptado em Estrasburgo em 28 de Janeiro de 2003.* Diário da República n.º 179/2009, Série I de 2009-09-15, páginas 6415 – 6421. https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/91-2009-489702

Resolução do Conselho de Ministros n.º 92/2019. (2019*). Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República n.º 108/2009, Série I de 2009-06-05, páginas 2888 – 2895. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Santos, R., Azevedo, J., & Pedro, L. (2016). Literacia(s) digital(ais): definições, perspetivas e desafios. *Media & Jornalismo*, *15*(27), 17–44. https://doi.org/10.14195/2183-5462_27_1

Sarmento e Castro, C. (2022). *Portugal assina protocolo adicional à Convenção sobre Cibercrime*. https://justica.gov.pt/Noticias/Portugal-assina-segundo-protocolo-adicional-a-Convencao-sobre-Cibercrime

Shukurov, E., & Jafarov, U. U. (2023). Legal Professionals' Perspectives on the Challenges of Cybercrime Legislation Enforcement. *Interdisciplinary Studies in Society, Law, and Politics*, *2*(4), 25–31. https://doi.org/10.61838/kman.isslp.2.4.5

Stefan, M. & Fuster, G. (2018). Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters State of the art and latest developments in the EU and the US. *CEPS paper in Liberty and Security*. https://www.researchgate.net/publication/329585231_Cross-border_Access_to_Electronic_Data_through_Judicial_Cooperation_in_Criminal_Matters_State_of_the_art_and_latest_developments_in_the_EU_and_the_US

Stol, W., Lentz, L., Naarttijärvi, M., Sunde, I., Jackson, A., Strikwerda, L. & Jansen, J. (eds.) (2025). *Legal and Ethical Issues in Digital Policing. Policing in the Digital*

*Society Network Yearbook 2025.* https://ris.utwente.nl/ws/portalfiles/portal/471521100/Legal_and_Ethical_Issues_in_Digital_Policing.pdf

United Nations Office on Drugs and Crime (UNODC) (2021). *Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020.* https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101012.pdf

Venâncio, P. D. (2011). *Lei do Cibercrime - Anotada e comentada.* Coimbra: Coimbra Editora.

Venâncio, P. D. (2021). Tipos Legais de Crimes Informáticos. Em I. Guedes, & M. Gomes, *Cibercriminalidade: Novos desafios, ofensas e soluções* (pp. 75-97). Lisboa: PACTOR.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Wall, D. (2017). Crime, security and information comunication technologies: The changing cibersecurity threat landscape and its implications for regulation and policing. Em S. Brownsword, & K. Yeung, *The Oxford Handbook of the Law and Regulation of Technology* (pp. 1075-1096). Oxford: Oxford University Press.

Whelan, C., Bright, D., & Martin, J. (2023). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology, 57*(1), 45-61. https://doi.org/10.1177/26338076231199793

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows: The police and neighborhood safety. *The Atlantic Monthly, 249*(3), 29–38.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.

World Economic Forum (2024). *Collaboration is key to tackling cybercrime. Recent takedowns show why.* https://www.weforum.org/stories/2024/11/collaboration-key-tackling-cybercrime-cybersecurity/

.PT (2024). .PT e PSP celebram protocolo para combate à cibercriminalidade. https://www.pt.pt/pt/noticias/pt-e-psp-celebram-protocolo-para-combate-a-cibercriminalidade/#:~:text=O%20.PT%20e%20a%20Pol%C3%ADcia%20de%20Seguran%C3%A7a,o%20aprofundamento%20m%C3%BAtuo%20das%20capacidades%20de%20ambas