ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P

VOL. 17 N. 2 [2023]

ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P
BI ANUAL | BI ANNUAL

DOUTRINA

SECÇÃO TEMÁTICA

Eduardo Fernández García

# Cibercrimes Contra a Segurança do Estado: Recomendações *De Lege Ferenda* Comparadas Entre Portugal e Espanha

CEAD FRANCISCO SUAREZ
Fdcp Faculdade de Direito e Ciência Política
UNIVERSIDADE LUSÓFONA | CENTRO UNIVERSITÁRIO PORTO

ULPLR

# CIBERCRIMES CONTRA A SEGURANÇA DO ESTADO: RECOMENDAÇÕES *DE LEGE FERENDA* COMPARADAS ENTRE PORTUGAL E ESPANHA[1]

EDUARDO FERNÁNDEZ GARCÍA[2]

DOI: 10.60543/UL-PLR-RDUL-P.V17I2.9508

**RESUMO**

As sociedades portuguesa e espanhola atuais caraterizam-se por uma profunda hiperconetividade. Boa parte da atividade transita já da realidade física para o mundo lógico. Portanto, devem enfrentar o aumento dos riscos e ameaças que pairam sobre a segurança pública e a segurança nacional na transição às relações cibernéticas. Há duas décadas, diferentes ramos do Direito passaram a interessar-se pelo ciberespaço. Com algumas implicações constitucionais de extraordinária importância, a cibersegurança está a ser regulada por normas administrativas em Portugal e Espanha, o que contrasta com a imutabilidade das leis penais. Embora o planeamento público tenha melhorado em ambos os países, um olhar crítico sobre os regulamentos positivos penais atuais produz resultados insatisfatórios. Propõe-se aqui uma metodologia interdisciplinar de análise de um conjunto de propostas legislativas, dado que a obsolescência do teor literal de alguns artigos escritos antes da existência de meios tecnológicos revela um aumento da vulnerabilidade social, que exige uma atualização para incorporar mudanças significativas na tipificação das condutas puníveis e na modulação da autoria e da cumplicidade. O particular caráter tuitivo do Direito Penal e a relevância das suas respostas jurídicas obriga a resistir às exigências dos setores técnicos que impliquem um maior populismo punitivo.

**PALAVRAS-CHAVE**

:

autoria, cibercrimes, Direito da cibersegurança, interdisciplinaridade jurídica, reforma legislativa.

**ABSTRACT**

Current Portuguese and Spanish societies are characterized by profound hyperconnectivity. A significant portion of activities has already shifted from the physical reality to the digital world. Therefore, they must face the increase in risks and threats that loom over public safety and national security in the transition to cyber relations. Two decades ago,

1 Este artigo faz parte de uma investigação de Direito comparado mediante uma estadia de investigação no Centro de Estudos Avançados em Direito Francisco Suárez da Universidade Lusófona no Porto. O autor agradece ao CEAD a sua hospitalidade e particularmente à Prof.ª Doutora Inês Godinho pela sua guia no Direito Penal português dos cibercrimes.

2 Professor Doutor de Direito Digital da Universidade Pontificia de Salamanca.
Email: efernandezga@upsa.es ORCID: https://orcid.org/0000-0002-9225-1071

various branches of law began to take an interest in cyberspace. With some extraordinarily important constitutional implications, cybersecurity is being regulated by administrative norms in Portugal and Spain, which contrasts with the immutability of criminal laws. Although public planning has improved in both countries, a critical glance at current positive penal regulations yields unsatisfactory results. An interdisciplinarity methodology for situation analysis and a set of legislative proposals is proposed here, as the obsolescence of the literal content of some articles written before the existence of technological means reveals a increase in social vulnerability, which requires an update to incorporate significant changes in the classification of punishable conduct and in the modulation of authorship and participation. The particular protective nature of Criminal Law and the relevance of its legal responses requires it to resist the demands from technical sectors that imply greater punitive populism.

*Keyword*: authorship, cybercrimes, Cybersecurity Law, legal interdisciplinarity, legislative reform.

Sumário: 1. Introdução: o Direito Digital e a função tutelar do Direito Penal sobre a cibersegurança nacional 2. Cibersegurança nacional desde a perspetiva penalista 3. Direito Penal e proteção integral dos bens jurídicos atinentes à segurança nacional 4. Uma proteção penal restrita 5. Propostas *de lege ferenda* 6. Conclusões 7. Bibliografia

## 1 INTRODUÇÃO: O DIREITO DIGITAL E A FUNÇÃO TUTELAR DO DIREITO PENAL SOBRE A SEGURANÇA NACIONAL

Os Códigos Penais português e espanhol obedecem a um similar enfoque para regular os tipos penais de espionagem e traição. Nos dois Códigos, entre os crimes contra a independência do Estado e a Defesa nacional. No caso português, no Título V Dos crimes contra o Estado, Capítulo I Dos crimes contra a segurança do Estado, Secção I Dos crimes contra a soberania nacional, Subsecção I Dos crimes contra a independência e a integridade nacionais, artigos 308 para a traição à pátria e 317 para a espionagem. No caso espanhol, no Título XXIII *De los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional*, Capítulos I *Delitos de traición, II Delitos que comprometen la paz o la independencia del Estado* e III *Del descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional*, principalmente artigos 582 e 583 para a traição, 584 e 592 para a espionagem.

Embora não sejam os únicos tipos penais estrategicamente considerados crimes contra a Segurança Nacional, são os mais perigosos para a integridade do Estado, razão pela qual também se incluem no âmbito castrense. Assim, no Código de Justiça Militar português no Título II Parte especial, Capítulo I Dos crimes contra a independência e a integridade nacionais, Secção I Traição, artigo 25 para a traição à Pátria; Secção II Violação de segredo, artigo 33 para a violação de segredo de Estado e artigo 34 para a espionagem. E no Código Penal Militar espanhol no Título I *Delitos contra la seguridad y defensa nacionales*, Capítulo I *Traición militar*, artigo 24; Capítulo II *Espionaje militar*, artigo 25 e Capítulo III *Revelación de secretos e informaciones relativas a la seguridad y defensa nacionales*, artigo 26.

Neste artigo, evitaremos a comparação diacrónica entre os dois Códigos Penais e limitar-nos-emos, por razões de extensão e delimitação epistémica a apontar a necessidade de uma nova abordagem do conjunto, já que as condutas típicas mostram uma redação centenária. Neste momento, é impensável que os crimes de espionagem possam ser cometidos através do roubo físico de documentos escritos, como na altura em que estes tipos criminosos foram incluídos nos dois Códigos, já que atualmente o armazenamento de dados não tem suporte físico, mesmo em discos rígidos de computador e, tanto o armazenamento quanto o gerenciamento

de dados e programas relacionados à Defesa e à Segurança nacionais ocorrem na nuvem. Portanto, as normas relativas à sua custódia por agências governamentais bem como as relativas à prevenção da vulneração com novos meios de ataque informático começaram a interessar ao Direito Digital, como uma ponte comum que liga diferentes ramos jurídicos que afetam a Segurança Nacional.

O surgimento do Direito Digital como um ramo disciplinarmente autónomo do Direito (Schwalbach, 2021, p. 33) está transido de dificuldades académicas para encaixar a sua novidade epistémica entre os ramos tradicionais, sem o reduzir a uma inovação metodológica (Sidorenko e von Arx, 2020, p. 33). A primeira dificuldade para lhe outorgar estatuto académico autónomo reside na sua excessiva dependência das inovações tecnológicas (Gutbrod, 2020, p. 22). A incorporação mais notável de conteúdos substantivos do Direito Digital tem estado relacionada com a ampliação de procedimentos, tecnologias e serviços digitais. Atualmente, passou de focar-se nas implicações da proteção de dados pessoais e das transações de comércio eletrónico no ciberespaço para o uso de *blockchains* para financiamento cibernético, a proteção de direitos subjetivos com o uso da Internet das Coisas (IoT) e, mais recentemente, para as implicações constitucionais graves e disruptivas da inteligência artificial, tudo isso em relação à capacidade, não apenas de armazenamento, mas de processamento massivo que o *big data* oferece.

Consequentemente, e enquanto não adquira maior autonomia disciplinar, o Direito Digital atua como complemento subsidiário do Direito Penal no que diz respeito à compreensão dos desenvolvimentos terminológicos e conceituais derivados da introdução de novas tecnologias, mas nunca no deslocamento da regulação substantiva do elemento objetivo dos tipos através da incorporação de meios comissivos tecnológicos. Se o Direito Digital não pode aspirar a uma intervenção tão invasiva, então seria aconselhável uma atualização do Direito Penal que tivesse mais em conta o impacto notável das tecnologias, após as primeiras hibridizações entre Direito Digital e Direito Penal e relação com crimes de conteúdo económico (Silva Rodrigues, 2009). Particularmente nas formas de comissão dos crimes, na sua tipologia e taxonomia no Código Penal, numa precisão adequada da cumplicidade e da comparticipação em relação à autoria. Além disso, para facilitar uma aplicação dinâmica da lei processual penal, devido à dificuldade de precisão do *locus delicti comissi* na transição entre a traçabilidade tecnológica e a imputação processual pela incidência da ubiquidade e a comissão a longa distância no princípio de aplicação da competência territorial das jurisdições portuguesa e espanhola para proferir despachos de pronúncia sobre atos cometidos no ciberespaço.

Em relação aos crimes contra a Segurança e a Defesa Nacionais, quando estas questões são contempladas no atual mundo *hipertécnico* em comparação com a antiguidade da literalidade dos artigos dos Códigos Penais português e espanhol, percebe-se que a conceção dos elementos objetivos do tipo se tornara obsoleta para formas comissivas no ciberespaço.

Sobre todos estes conteúdos está a ser promovida uma investigação jurídica intensa, embora apoiada na multidisciplinaridade com outras Ciências Sociais e com as Ciências da Computação e também na interdisciplinaridade jurídica. Esta última revela que tanto o Direito Administrativo como o Direito Penal prestam cada vez mais atenção a alguns aspetos substantivos que variam na sua essência ou natureza jurídica com a mudança das tecnologias de utilização, que no caso do Direito Penal se referem à comissão dos crimes. Como as modalidades de comissão dos crimes afetam subsequentemente a conceção da autoria, parece estar já ultrapassado o tempo de uma autorregulação voluntarista como a que propôs a *Estratégia Digital Europeia, Regulação e garantias constitucionais.*

Estes tipos penais não são frequentemente estudados ou atualizados pelos legisladores nacionais, quer porque o poder público não deseja transmitir uma sensação de vulnerabilidade das estruturas do Estado, quer porque foram regulamentados criminalmente sob o pressuposto de não haver produção prática. Esta suposição de uma comissão muito residual em relação a todos os crimes contra a segurança parecia apoiada pela análise jurisprudencial e pela escassez de processos penais incoados para processar aqueles que possam ter cometido crimes de traição e espionagem. Porém, esta visão quantitativa do problema deveria ser modulada a curto prazo por dois motivos: basta que seja cometido um ataque cibernético de notável efetividade contra as infraestruturas críticas para que a vulneração dos bens jurídicos a serem protegidos seja muito maior que no caso de muitos crimes de violação de segredos de menor importância; além disso, existe atualmente uma maior lassidão na acusação nos crimes cometidos no ciberespaço devido à complexidade técnica da identificação dos arguidos.

Duas razões com impacto idêntico nos países do âmbito comunitário e da OTAN recomendam a alteração da atual regulamentação dos crimes de traição e espionagem em Portugal e Espanha. Por um lado, os meios de comissão informáticos são ignorados ou desatualizados em ambos os Códigos Penais e é imperativo incorporar o impacto do ciberespaço e das ferramentas digitais na comissão destes crimes, o que afeta a conduta como elemento objetivo dos crimes, mas modifica algumas conceções tradicionais de autoria. Este impacto inegável aconselha modular a dogmática penal, considerada esclerosada desde o Direito Digital, destes tipos penais nos dois Códigos à luz de critérios de política criminal.

Por outro, as sociedades portuguesa e espanhola caraterizam-se pela sua abertura ilimitada ao mundo e por receberem os efeitos da globalização que afeta também a Segurança Nacional, como afetou a Segurança Pública quando se decidiu introduzir em ambos os países algumas figuras de cibercrimes contra bens económicos ou contra a liberdade sexual. Em momentos de intensa conflitualidade global não parece que a Segurança Nacional deva estar mais desprotegida que a Segurança Pública, quando são propostas novas regulamentações de proteção no setor público dos serviços governamentais que utilizam *blockchains* (Meirelles Magalhães, 2021, p. 17).

Este artigo critica a inadequação e obsolescência da regulamentação positiva dos ilícitos penais nos Códigos de ambos os países, mas não se contenta com censurar a despreocupação do legislador em relação à proteção da Segurança Nacional no ciberespaço. As Estratégias de Segurança Nacional há cinco anos consideravam as pandemias como uma das principais ameaças às sociedades permeáveis como as ibéricas, e por mais que se proclamasse a existência teórica de uma vulnerabilidade para a qual se dizia que as estratégias nacionais incluíam algumas previsões, a prática demonstrou durante a pandemia de COVID-19 a insuficiência da capacidade protetiva do Direito Público, especialmente do Direito Administrativo. Pois bem, as Estratégias Nacionais hoje consideram que uma das principais vulnerabilidades, se não a maior, é a crescente desproteção do ciberespaço e, as sociedades portuguesa e espanhola, menos confiantes agora, esperam uma capacidade tutelar eficaz e real do Direito Penal. Por esta razão, uma parte fundamental deste artigo estriba na proposta de algumas reformas imediatas da regulamentação penal, que serão insuficientes por si só se não forem acompanhadas de reformas simultâneas das leis processuais e sem o acompanhamento de uma visão mais pró-ativa do Direito Constitucional e mais eficiente do Direito Administrativo. O ponto de partida legal é a impossibilidade tecnológica do risco zero, ainda que a sua redução seja o objetivo da hipertrofia da lei sancionadora (Vilela, 2022, p. 92).

O Direito Penal está ciente da irrupção de novos problemas jurídicos derivados das inovações informáticas: algoritmos e decisões automatizadas, engenharia social, campanhas de desinformação à escala massiva, ou inexistência de uma sorte de *compliance* digital. Todas estas transformações tecnológicas, já estudadas pelo Direito Digital, obrigam-nos a propor ao Direito Penal a conveniência de repensar o âmbito da autoria: quem é o autor no caso de ataques cibernéticos causados por algoritmos criados por modificação automática através de *Deep Learning* em que não há intervenção humana nas últimas transformações informáticas que levam à perfeição do ataque (Aires de Sousa, 2020, p. 60)? Existe responsabilidade criminal no caso de uma estratégia deliberada de desinformação que dê origem a agitação e revoltas sociais? Os fornecedores digitais, prestadores de serviços informáticos e provedores de ligações à *Internet* têm algum tipo de responsabilidade criminal no caso de vulnerabilidades persistentes corrigíveis que permitam a sua utilização para ações criminosas? São questões que estão no debate social, no confronto parlamentar e nas reflexões éticas, mas que têm um alcance penal inegável no curto prazo, embora, pela sua natureza altamente coercitiva, a norma penal deva dotar-se de uma especial cautela e ponderação dos interesses sociais.

Enfrentá-las de forma decisiva é mais importante neste momento do que nos períodos anteriores em que os usos da espionagem pareciam esquecidos durante décadas, até que chegaram os problemas de intensificação dos ataques cibernéticos como consequência da guerra na Ucrânia e do jihadismo *online*. O *Relatório Cibersegurança em Portugal 2023* do Centro Nacional de Cibersegurança, organismo do governo, afirma na página 9 "Os atores estatais e paraestatais também desenvolveram atuações maliciosas no ciberespaço de interesse nacional, nomeadamente de ciberespionagem. Algumas destas ações enquadraram-se no contexto da guerra na Ucrânia e respetivos antagonismos geoestratégicos. Também fruto deste contexto, verificou-se a existência de ações de grupos *hacktivistas*, de cunho patriótico, que procuraram impactos mediáticos de modo a afirmarem a sua causa e ideologia, tendo em conta o alinhamento político de Portugal nesta matéria".

Além disso, não parece que o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial recém-aprovado possa efetivamente garantir a limitação do *software* de inteligência artificial de *deep learning*. Especialmente se os seus algoritmos puderem auto adaptar-se para eludir os mandatos legais (Fernandes Godinho et al., 2020, p. 165) para que não violem direitos fundamentais de potenciais vítimas com uma posição particularmente relevante para a segurança nacional. Em relação ao sigilo das suas comunicações, isso pode resultar em ilícitos penais concretizados no tipo de espionagem regulada pelos artigos 316 e 317 do Código Penal Português (CPP) e 598 e 599 do Código Penal Espanhol (CPE).

## 2. CIBER-SEGURANÇA NACIONAL DESDE A PERSPETIVA PENALISTA

É importante lembrar que os desafios jurídicos da segurança cibernética nos dois países não são menores que os desafios tecnológicos, mas ocorrem com um desfasamento maior entre a necessidade social e a resposta legislativa. Este contexto é particularmente preocupante em relação à segurança nacional e à segurança de infraestruturas críticas, ambas no ciberespaço. Defende-se aqui uma mudança na mentalidade com que se empreende o processo de reforma legal a este respeito em dois sentidos: por um lado, uma maior necessidade de interdisciplinaridade do que a utilizada para modificações legislativas noutros ramos do Direito Público; por outro, maior celeridade para acompanhar o ritmo vertiginoso a que se produzem as modificações

dos instrumentos tecnológicos para a prática de atos ilícitos administrativos e penais.

Muitos órgãos das Administrações, das Forças de Segurança e das Forças Armadas lidam com essas questões, não fosse a notável incidência disruptiva que os cibercrimes têm nas sociedades portuguesa e espanhola, também para a segurança nacional. Paradoxalmente, face a esta especialização orgânica e funcional essencial nos dois países, verifica-se uma considerável inércia dos ordenamentos jurídicos no que diz respeito à proteção penal da segurança nacional. Com atenção escrupulosa às exigências constitucionais (Barcelar Gouveia, 2022, p. 86) na monitoração (Álvarez Rodríguez, 2019, pp. 21–46; Neiva, 2021, p. 65) e, apesar de uns inícios titubeantes (Gutiérrez Espada, 2020, p. 226), o Direito regulador da segurança pública, cidadã e nacional acomodou-se a essa evolução (Suñé Llinas, 2007) com um elevado grau de especialização, mas com tempos muito diferentes dos das inovações técnicas.

A tendência incremental à hiperconetividade (Gómez de Ágreda, 2021, p. 30; Goncalves e Mascarello Luciani, 2023, p. 1130) que caraterizava as sociedades portuguesa e espanhola nos últimos cinco anos intensificou-se devido às restrições de mobilidade e conexão física introduzidas normativamente como consequência das recomendações sanitárias de distanciamento social devido à pandemia de COVID-19. Os requerimentos acumulados na esfera técnica e na dimensão jurídica requerem o acompanhamento de dois paradigmas altamente exigentes. Por um lado, o que se forjava como um diferente ambiente de relações sociais e económicas ao qual deveria adaptar-se o ordenamento jurídico tornou-se um condicionante absoluto para o atual paradigma da segurança integral que afeta, simultaneamente, a dimensão interna e externa ou internacional que devem ser protegidas do ponto de vista jurídico (Fernández Bermejo e Martínez Atienza, 2018, p. 88). Empresas e Administrações tiveram de aclimatizar-se a esta conjuntura, e parecem fazê-lo melhor as primeiras que as segundas, provavelmente porque os instrumentos para implementar novas medidas são de natureza muito diferente: planos no caso das empresas, normas jurídicas no das Administrações Públicas. Por outro lado, do novo paradigma da omniconetividade permanente resultou a correlativa necessidade de mecanismos jurídicos que protejam os direitos constitucionais, tanto contra eventuais excessos e ataques anti-jurídicos que possibilitam o uso irrestrito de tecnologias disruptivas -mas ao mesmo tempo invasivas-, como face aos mecanismos telemáticos igualmente amplos dos poderes públicos na perseguição dos cibercrimes.

Do pedido dos setores técnicos para atualizar as leis e regulamentos que regem o Direito da Cibersegurança passou-se a uma necessidade social amplamente sentida, o que exige uma rápida atualização das principais normas, tanto administrativas como penais e processuais. Quando já começam a circular propostas concretas e se sugere dar forma a textos articulados que passarão ao Parlamento entre a presente legislatura nacional e a seguinte, convém sublinhar a necessidade das reformas legislativas previstas se adaptarem a uma realidade social e tecnológica extraordinariamente mutável em apenas um lustro. Esta realidade não conhece compartimentos estanques, nem entre parcelas sociais afetadas -económicas, jurídicas, éticas, técnicas-, nem entre países. O anonimato e a longa distância em que se cometem os ciberataques dão conta intuitiva das dificuldades que enfrentam o Direito Penal e o Direito Processual Penal. Ao primeiro, exigem-se respostas mais ágeis do que as previstas para os cibercrimes de novo cunho introduzidos até agora na Lei 109/2009 do Cibercrime e na reforma do CPE da Lei Orgânica 5/2010. Ao segundo, uma eficácia na perseguição do crime dentro do necessário contexto de garantia dos direitos constitucionalmente consagrados, que está a ser mal ensaiado através da cooperação judiciária internacional.

De notar a enorme disparidade entre os ciberataques e os ciberincidentes geridos pelos serviços públicos e os

processos penais instruídos que passam das fases preliminares ao inquérito. No ano 2023, o Centro Nacional de Cibersegurança português registou perto de três mil denúncias de cibercrimes, um crescimento, de 60% face ao ano anterior. Seria irreal pensar que a quantidade de denúncias ao Gabinete Cibercrime da Procuradoria-Geral da República diminuísse face a anos anteriores, como desvela o número de ciberataques atendidos pela Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) e a modificação da metodologia de quantificação. Mas o problema mais preocupante não é o número de ataques cibernéticos, mas sim os meios de os cometer que afetam a sua eficácia. O último relatório oficial governamental português reconhece uma frequência elevada como prática dos agentes de ameaça em causa em Portugal protagonizados por "atores estatais", para utilizar a mesma terminologia oficial, em *phishing*, *smishing* e *vishing*, em comprometimento de contas, em cibersabotagens de indisponibilidade, em distribuição de *malware*, em exploração de vulnerabilidades e, em ciberespionagem. Pode o Direito Penal dar-se ao luxo de não tipificar as condutas mais perigosas quando estas afetam infra-estruturas críticas e o alvo principal dos ataques não é a Administração Pública, mas a mesma sociedade portuguesa no desfrute dos seus direitos constitucionais? Sobretudo porque o mesmo relatório do governo afirmava que as ameaças do contexto geopolítico e estratégico constituem um cenário persistente (p. 14).

O panorama é similar no caso espanhol: o Incibe (*Instituto Nacional de Ciberseguridad* espanhol) comunicou mais de cento e trinta mil incidentes enquanto os processos judiciais abertos na ordem penal por cibercrimes, que apesar de terem aumentado, apenas passam dos onze mil e as sentenças condenatórias penais ficam em mil. Esta diferença nos números revela a existência de uma vasta zona cinzenta de elevada impunidade que conviria ser reduzida para evitar que a incidência na dimensão económica seja maior, minando a confiança do consumidor e a segurança jurídica das transações *online* que o Direito Comercial havia conseguido introduzir normativamente em Espanha, em Portugal e no ordenamento comunitário.

## 3. DIREITO PENAL E PROTEÇÃO INTEGRAL DOS BENS JURÍDICOS ATINENTES À SEGURANÇA NACIONAL

A principal reclamação aqui contida na hora de abordar a reforma legal penal futura da cibersegurança nacional em Espanha e em Portugal é que se vincule a uma compreensão global e integral. Trata-se, assim, de uma noção suscetível de proteger a sociedade contra as ameaças e ilícitos penais provenientes de todo o mundo e em todos os setores da atividade social da segurança nacional, que constitui afinal, um único, embora poliédrico, bem legal a proteger. Esta exigência genérica traduz-se nas aludidas duas exigências simultâneas de multidisciplinaridade entre o Direito e outras ciências e saberes e, de interdisciplinaridade entre diferentes ramos jurídicos, que vão além da tradicional extensão da resposta penal à prevenção administrativa, passando por exigências de agilidade processual que dificilmente podem ser resolvidas na ótica de um único país. Vejamos estes três aspetos e as suas implicações antes de passarmos a propostas de reforma jurídica concretas.

Primeiro, há algumas precisões sobre a essência do bem jurídico vulnerável. Devido à intangibilidade do ciberespaço e à sua vasta quantidade de conteúdos, dados e ações possíveis, é inviável abrangê-lo todo, especialmente no que diz respeito às fronteiras. Se esta foi a consideração inicial em momentos de menor extensão lógica do ciberespaço (González Hurtado, 2014, p. 4), já não é possível se ponderarmos a incomensurabilidade dos dados disponíveis, os intercâmbios informáticos realizados diariamente e a expansão da capacidade de processamento mundial que cresce

exponencialmente. O aparente impasse da famosa Lei de *Moore* sobre a duplicação da capacidade dos *chips* dos microprocessadores a cada dois anos já não é o problema; nem é a abordagem adequada à escala global quando se tem em conta a inter-relação entre mineração de dados setorizada, *blockchains* (Moret Millás, 2020, p. 97; Requena Jiménez, 2017, p. 114), Internet das Coisas e Inteligência Artificial (Arteaga Martín, 2019, pp. 154–160; Cubeiro Cabello, 2020, p. 99; Fuente Chacón, 2019, pp. 70–72; Valls Estefanell, 2018, pp. 272–275). Particularmente relevante é esta última dimensão, que ameaça incorporar-se mediante um potencial uso autónomo de armas (Lemos e Costa, 2022, p. 92) e ciberarmas através de programas automatizados sem a intervenção humana (Márquez Díaz, 2017, p. 49; Singer, 2015, p. 43). Ainda, o principal problema atual foca-se na gestão de *big data*, que foi iniciada como segurança dos dados que podem ser exigidos na defesa nacional (Aldana Montes et al., 2018; Navarro, 2016, p. 8) e é desenvolvido especificamente como *big data* aplicada à segurança nacional e à defesa (Alcantarilla, 2016; Carrillo Ruiz et al., 2013, p. 48; Malhado, 2017, p. 42)

Segundo, mais inadequada é uma visão do bem jurídico transida de componentes puramente tecnológicos. É inviável transferir para o âmbito jurídico a conceção técnica estreita de proteção da confidencialidade, integridade e disponibilidade das redes. Dado que é impossível, no momento atual, limitar o crescimento do ciberespaço a relações sociais e jurídicas anteriormente não reguladas pelo ordenamento, os riscos e ameaças decorrentes do aumento das vulnerabilidades introduzidas por esse alargamento devem ser incorporados no bem jurídico protegido.

Compreendem-se as complexas implicações dessa visão esférica do bem jurídico a proteger ao considerar que não são intercambiáveis as categorias de ciberincidente, ciberataque, cibercrime e comissionamento por meios telemáticos de outros delitos, claro, todos eles projetados exclusivamente sobre a segurança nacional. Quando se analisa separadamente o total das ocorrências registadas, estudadas e classificadas pelo Centro Nacional de Cibersegurança em Portugal e pelos Incibe e Centro Criptológico Nacional em Espanha, percebe-se que os fenómenos a que se refere este artigo são unicamente ciberataques e delitos de espionagem e sabotagem cometidos por meios telemáticos.

A frequente controvérsia sobre o bem jurídico a proteger não pode ser resolvida de forma restrita para o vincular de maneira exclusiva à integridade do Estado e às suas manifestações de soberania, que era a perspetiva dogmática do tempo da codificação. Isto tem acontecido ao contemplar os tipos penais dos delitos do título XXIII do CPE e do Título I do Livro II do Código Penal Militar espanhol, delitos todos eles atinentes à espionagem ou à traição, desde a rubrica da paz, a independência e a Defesa do Estado, que se traduz também no Código Penal Militar em segurança do Estado. São tipos penais similares aos regulados no CPP nos já citados artigos 308 de traição à pátria e 317 de espionagem, aos quais haveria de adicionar-se, no caso português o artigo 329 relativo à sabotagem e, na atual redação do Código de Justiça Militar português nas secções I e II dos crimes contra a independência e a integridade nacionais, que desenvolvem mais pormenorizadamente os crimes de traição, espionagem e violação de segredos, num sentido ainda mais elaborado dogmaticamente do que noutros países no entorno de segurança comum, como a França e a Itália, e especialmente como o Reino Unido ou os Estados Unidos.

Por um lado, o bem jurídico a proteger não é exclusivamente o ciberespaço como domínio operacional da segurança. Por outro, não podem ser unicamente parcelas como a paz ou a independência de Portugal e Espanha que, por mais relevantes que sejam individualmente, devem ser consideradas conjuntamente como contexto do normal desenvolvimento da sociedade. Ainda menos os planos, documentos ou objetos que estão na literalidade do artigo 317 CPP ou 600

CPE. Deve considerar-se a informação classificada, reservada ou secreta como no artigo 598 CPE.

Esta foi a consideração habitual ao enfrentar o relato dos bens jurídicos considerados um a um em cada tipo penal dos crimes de espionagem, sabotagem e violação de segredo. Esta perspetiva dogmática revela-se insuficiente ao atender ao objeto final da proteção integral de Espanha e Portugal como Estados independentes, mas das sociedades ibéricas como comunidades ativas, protagonistas do exercício dos direitos fundamentais. Compreende-se esta ideia ao considerar que nas Constituições, portuguesa (no artigo 27) e espanhola (no artigo 17), o legislador constituinte erige a dupla liberdade / segurança em uníssono.

Muitas vezes a perspetiva dogmática levou a erigir a precisão sobre o bem jurídico como o núcleo central sobre o qual gira toda a segurança. É o que tem acontecido na configuração dos cibercrimes, e parece que neste momento estão em causa quaisquer reformas que aumentem a proteção no ciberespaço. Este procedimento que parte sempre do bem jurídico apresenta, no entanto, na atual demanda social, dois inconvenientes. Primeiro, é excessivamente tributário de uma perspetiva penalista punitiva, que não tem igual utilidade na dimensão preventiva e dissuasora do Direito Penal. Segundo, o desbordamento dos limites conhecidos que a tecnologia possibilita atinge também esta questão, sendo difícil identificar um único bem jurídico a proteger quando os ciberataques afetam, simultaneamente, infraestruturas materiais, serviços intangíveis e direitos relacionados com ambos.

## 4. UMA PROTEÇÃO PENAL RESTRITA

A partir da especial consideração do ciberespaço como *locus delicti commisi*, é necessário ampliar a abordagem jurídica para as reformas de outros setores do ordenamento que já se anunciam. Este artigo menciona algumas propostas concretas de *lege ferenda* para esse imediato e imprescindível processo e elabora-as a partir da dupla premissa epistémica na preparação técnica dos anteprojetos de lei.

A par da multidisciplinaridade na elaboração dos textos articulados e do conjunto de relatórios prévios que devem dar forma nos primeiros passos do iter legislativo, aos anteprojetos de lei, postula-se aqui a necessidade de interdisciplinaridade jurídica. Especialmente porque existem limites fixados tanto pelo Direito Constitucional como pelo Direito Internacional Público. Para que disciplinas como o Direito Administrativo, o Direito Penal e o Direito Processual, com seus objetos de estudo bem estabelecidos, possam convergir num mesmo campo analítico, é necessário estabelecer previamente mecanismos normativos de comunicação. Fazê-lo pausadamente e com consenso, em vez de mediante a habitual fórmula das leis *omnibus* que tanta improvisação e aleatoriedade introduziram em alguns setores do Direito Administrativo, o que projetado no âmbito penal não implicaria senão desproteção e discricionariedade de graves implicações constitucionais. Embora os primeiros passos para incorporar nas normas de segurança as conexões entre o mundo físico e o lógico, e como estas influenciam a natureza dos ilícitos (González Rus, 2006, pp. 241–250), tenham sido dados, o conjunto completo de exigências demandado pela visão holística incorporada na LSN ainda não foi totalmente retomado.

Pode argumentar-se que a natureza especial da norma penal requer um encaminhamento *ad hoc* que impede a penetração de outras perspetivas jurídicas mais laxas, que são as que neste momento traçam as conexões e a delimitação entre segurança global, segurança pública e segurança nacional. Este artigo foca-se particularmente na última, mas é impossível hoje restringi-la de tal modo que não tenha intensas ligações tutelares com uma segurança integral que abraça simultaneamente aspetos administrativos e penais.

Ao criticar o desfasamento existente na legislação penal no que diz respeito à dissuasão preventiva no ciberespaço da comissão de crimes contra a Defesa e Segurança nacionais, são quatro as questões a considerar em relação a uma possível reforma legislativa dos crimes cibernéticos: em primeiro lugar, a distinção entre cibercrimes em sentido jurídico estrito e crimes cometidos com uma camada cibernética; segundo, se a utilização de meios informatizados de comissão modifica a conduta a tal ponto que as atuais descrições das ações puníveis nos Códigos Penais sejam insuficientes; terceiro, se a utilização de meios tecnológicos de terceiros (desenvolvimento de *software* e de algoritmos adaptativos, programas de acesso à *deep web* e à *dark web* e disponibilização de ligação de via fibra ótica ou cobertura de satélite) afeta uma regulação da autoria nos dois Códigos ancorada nas formas de comissão pessoal no mundo presencial; por último, o impacto que o lugar de comissão do crime transnacional no ciberespaço pode ter nos aspetos criminais da imputação mais diretamente relacionados com os requisitos processuais e o princípio de territorialidade da lei penal em Portugal e Espanha.

Ainda que para o Direito Penal seja possível contemplar o ciberespaço (Picotti, 2019, p. 1292) no seu conjunto e não apenas para efeitos da utilização de métodos de comissão telemáticos dos delitos, no domínio da proteção penal da segurança nacional não se registou um esforço de adaptação das normas semelhante ao que foi feito para a segurança pública. Nas mais recentes reformas, foi-se dando lugar à progressiva contemplação do uso das novas tecnologias da telecomunicação e das novas ferramentas informáticas para a comissão dolosa de factos típicos que já estavam contemplados no Código Penal e de novos ilícitos. Em relação aos primeiros, a camada ciber utilizada para a comissão variava parcialmente alguns elementos objetivos dos tipos penais, como se observa particularmente no caso de fraudes ou apropriações indevidas; em relação aos segundos, a mudança de visão introduzida para as ciberburlas e crimes de conteúdo patrimonial no ciberespaço parece ser um modelo adequado, embora insuficiente.

Todos eles incorporaram uma dupla novidade: a existência do ciberespaço como lugar de comissão dos delitos e a imprescindível utilização de meios telemáticos nas modalidades de comissão mais tecnificadas. Nada disto está presente à letra nos Códigos Penais ou nos Códigos de Justiça Militar para as infrações relacionadas com a segurança nacional. Se atendermos à redação de todos os artigos e se considerarmos o traçado histórico, surpreende negativamente a invariável literalidade de muitos deles desde há muitas décadas. Em nome da necessária concisão não é possível abordá-los aqui, mas quando se analisam os delitos de traição, espionagem, ingerência na soberania ou revelação de segredos relativos à Defesa Nacional, todos vinculados com a segurança nacional, reconhece-se que hoje se mantém o conceito de infraestruturas essenciais para a segurança que estava em vigor nos códigos do século XIX. Se tivermos em conta que a incorporação das últimas infraestruturas suscetíveis de serem atacadas para enfraquecer a segurança nacional eram os aeródromos, compreende-se o desfasamento que impede relacionar qualquer perspetiva de cibersegurança com a segurança nacional apreciada penalmente. Consideremos como possíveis exemplos as novidades incluídas para os delitos de interceção das transmissões de dados, os delitos informáticos relacionados com a propriedade intelectual e industrial e os de intrusão informática.

Os inconvenientes não são apenas de natureza dogmática. O maior obstáculo a atribuir à lei penal para proporcionar uma proteção adequada no ciberespaço à segurança nacional deriva principalmente da distância que se sente entre os meios tecnológicos e a finalidade de política criminal que deveria perseguir uma regulamentação mais atualizada e realista. Esta deveria ser a orientação que poderia ser dada a uma nova redação dos artigos do título XXIII CP

para melhor apreciar a singularidade do elemento objetivo do tipo (Serrano Ferrer, 2016, Capítulo 2 *Internet como medio comisivo*). Assim, da mesma forma que se afirmou com caráter geral, a perspetiva penal está necessitada de pontes interdisciplinares (Arias Holguín, 2018, p. 50) para uma proteção integral da segurança nacional. De forma particularmente intensa projeta-se aqui a insuficiência, até este momento, na passagem de uma visão dogmática para outra de política criminal mais compreensiva e ampla, que acrescente o campo de proteção que sociedades tão abertas como a portuguesa e a espanhola colocam neste momento como desafio principal para os poderes públicos (Miró Llinares, 2012, pp. 191–195).

Com particular ligação à perspetiva penal surgem severas restrições e inconvenientes derivados das exigências processuais e da inexistência de normas de autêntica projeção internacional ou transnacional. Além disso, as tentativas até agora promovidas por algumas organizações internacionais são de âmbito territorial limitado e de escassa especialização temática.

## 5. PROPOSTAS *DE LEGE FERENDA*

Dado que a regulamentação atual é parcial, insuficiente e, de certo modo, obsoleta, torna-se imprescindível implementar algumas reformas legislativas de grande envergadura e nos tempos politicamente comprometidos. Estes parecem ter sido modificados pelas alterações de prioridades introduzidas pela pandemia de COVID-19; mas seria um erro aproveitar a ocasião para adiar a resolução das mais graves disfunções já detetadas e unanimemente criticadas pelos operadores técnicos e jurídicos da cibersegurança. A intensificação dos ciberataques sofridos por utilizadores domésticos e empresariais empalidece perante a profundidade e a notoriedade mediática dos sofridos pelo setor público estatal e autónomo durante as épocas de mais severa restrição durante os sucessivos estados de alarme, como os ataques de *ransomware* sobre a rede de hospitais públicos e a paralisação dos serviços do Serviço Público de Emprego do Estado que se revelaram irremediáveis. Neste momento, os ciberatacantes de todas as condições, presumivelmente também aqueles que podem servir interesses de países fora da esfera das liberdades da UE, não cessaram os seus esforços para paralisar o normal desenvolvimento dos serviços públicos essenciais nem mesmo para entravar a operacionalidade das forças de segurança. Por conseguinte, longe de aliviar a necessidade de um ordenamento atualizado e robusto, este encontra-se no ponto mais alto desde a multiplicação dos ataques às infraestruturas críticas.

A enorme diferença entre os ataques na *Internet* e os processos em curso no âmbito do Tribunal Penal demonstra a insubstancialidade da legislação vigente, ao mesmo tempo que suscita um debate pouco sugerido hoje em sede parlamentar sobre a extensão da lei penal: primeiro, a inadequação e obsolescência de alguns elementos objetivos dos tipos atuais; segundo, o debate sobre os tipos penais abertos ou fechados nos delitos contra a segurança nacional, a independência do estado, a paz e, a Defesa nacional; terceiro, em que medida se dilui o esquema da autoria pelos condicionalismos de rastreabilidade em delitos cometidos a longa distância e por meios humanos e materiais interpostos ou mediatos.

As complicações derivadas da teoria roxiniana do domínio do facto introduziram um certo relaxamento das exigências do pensamento causalista anterior, prevalecente em Espanha e Portugal. Se podemos afirmar cada vez menos que o crime é um ato jurídico de natureza individual na dimensão presencial, então é impossível na dimensão digital.

A primeira questão refere-se à inadequação da regulação de determinados comportamentos que impedem proporcionar certezas sobre a proteção da segurança nacional comprometida na projeção externa do Estado pela presença em organizações e teatros de operações com regras diferentes

da nossa, ou sob o comando direto de organizações internacionais com diferente ordenamento jurídico diretor das suas operações, ainda que exista uma autorização ou mandato parlamentar em Espanha.

Os crimes de espionagem, revelação de segredos e traição deveriam ver a sua redação corrigida (Navarro Bonilla, 2014, pp. 2–9) para acolher as modalidades comissivas no ciberespaço ou com utilização de meios telemáticos. Estas modalidades alteram a autoria do responsável final do dano em relação ao provedor de instrumentos informáticos, especialmente se implicam controle humano dos meios automáticos (Romeo Casabona, 2022, p. 14). É difícil imaginar uma exfiltração de informação contida em papel, num momento em que foi digitalizada desde a cartografia até às ferramentas de ataque e defesa. No entanto, o nosso Código Penal continua ancorado numa redação anterior à máquina de escrever. Em rigor, não deveríamos falar de cibercrimes, mas de crimes com componente digital.

Isto leva os operadores jurídicos que não são especialistas em Direito Penal a priorizar uma visão destes tipos como crimes de resultado. Dado que a mera utilização de meios informáticos não pode constituir crime em si, quando a sua utilização conduz a um resultado semelhante ao tradicionalmente alcançado através da apropriação de documentos, estaríamos perante estes crimes. Mas esta perspetiva amplifica a falta de proteção dos serviços essenciais ao permitir maior impunidade à tentativa do artigo 22 CPP e do artigo 16 CPE. Para além disso, o conhecimento dos dados reservados ainda não seria considerado adequadamente enquanto não houvesse apropriação ou desaparecimento dos seus meios de suporte físico ou digital. Assim, parece mais adequado modificar a redação literal dos artigos para incluir a divulgação de dados e informações além da apropriação dos seus meios de comunicação. Só assim será possível contemplar algumas condutas que ultrapassam, em muito, a sanção administrativa quando os ataques de engenharia social, como o *phishing*, começarem a contar com ferramentas de inteligência artificial, ou a aquisição de informações provier do *hacking* de dispositivos *IoT* para uso policial, militar ou de inteligência. Especialmente quando se multiplica o *ransomware as a service* até que todas as redes governamentais sejam plataformas *XDR* (Deteção e Resposta Alargadas) e o reforço do *DevSecOps* (Desenvolvimento, Segurança e Operações) permita uma gestão mais confiável dos ecossistemas *multicloud*.

Para todos esses desafios deve preparar-se o Direito Penal no contexto dos novos eventos regulatórios de 2024 e 2025: o limite para transposição ao ordenamento nacional português da diretiva NIS2, aplicação do Decreto-Lei 65/2021 do Regime Jurídico da Segurança do Ciberespaço à Administração Pública portuguesa, a conformidade ao Regulamento Europeu *DORA* (*Digital Operational Resilience Act*), a conformidade da *Cyber Resilience Act*, o começo da aplicação da *Artificial Intelligence Act*, a aplicação em Portugal do esquema de certificação do *Cybersecurity Scheme on Common Criteria* e a aplicação das novas regras de *Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure*.

Como delimitar casos muito frequentes de coautoria e de autoria mediata, mais que de cumplicidade, que exigem necessariamente uma acumulação de atos, se alguns deles são automatizados na programação informática e não se desenvolvem com total conhecimento dos intervenientes na execução? Como modular o fundamento último da punição do participante nestas modalidades de comissão telemática a longa distância e com extraterritorialidade, especialmente em casos de acessoriedade qualitativa? Como contemplar a cooperação necessária, imprescindível, dos técnicos que ativam redes, mas não lançam o ciberataque? Como limitar devidamente o *iter criminis* especial destes crimes no ciberespaço com uma visão obsoleta de um direito penal do inimigo que é hoje inconciliável com a capacidade tecnológica? Este não é o lugar para discutir propostas de redação que caberão ao legislador, ouvidos os peritos técnicos, mas

de afirmar que não se admitem mais atrasos nesta reforma, considerando as graves falhas de segurança nacional causadas por casos notórios e mediáticos de fugas, que afetaram os nossos aliados atlânticos.

Alguns dos episódios, abaixo referidos, de interferência no normal desenvolvimento dos processos democráticos eleitorais nos países europeus, tiveram origem na Rússia, mesmo sem antecipar o eventual envolvimento de alguns aparelhos de inteligência do Kremlin. Os com maior impacto não o fizeram penetrando as redes militares de Espanha, França, Reino Unido, Itália ou Alemanha, mas agitando as opiniões públicas face a acontecimentos pontuais que geraram um enorme mal-estar. Trata-se de processos deliberadamente promovidos que, tendo em conta as legislações nacionais penais dos países afetados, se revelaram suscetíveis de perseguição por comissão dolosa de diversos ilícitos penais relacionados com a sedição, a independência externa do Estado pelos crimes eleitorais e, que tinham sido perpetrados através de uma engenharia social (Alonso García, 2015; Miceli et al., 2017; Periago Morant, 2019, p. 489) ainda necessitada de regulação específica.

Exige o ciberespaço e as modalidades comissivas telemáticas das ameaças híbridas uma maior generalização de tipos penais abertos? Trata-se de um debate em curso que deveria manter-se nos estritos termos jurídicos de delimitação da autoria e não abrir inconvenientes contaminações políticas perante a possibilidade de mudar alguns elementos objetivos nos delitos contra a segurança nacional e a independência do Estado. A pressão dos operadores técnicos aponta sempre para a abertura dos tipos penais, o que não é apenas uma preocupação relacionada com os crimes contra a segurança nacional (Torío López, 1995, p. 8). No entanto, este artigo não aponta para essa linha ao reivindicar uma maior juridificação das estratégias de segurança nacional, porque o conjunto de direitos é tão sensível que pode ser afetado pela aplicação das situações de interesse para a segurança nacional referidas nos artigos 23 e 24 da LSN espanhola, que dificultaria a perseguição penal de certos comportamentos que se referem à habilitação do substrato tecnológico utilizado para a prática do delito (Gorra, 2014, pp. 199–204).

Dada a impossibilidade de promover um direito global que permita a jurisdição universal, uma proposta excessivamente utópica neste momento (Hörnle, 2020, p. 15), são quatro as principais sugestões neste contexto: primeiro, um desejável mimetismo entre rastreabilidade tecnológica e nexo causal da imputação; segundo, um melhor tratamento das implicações da transnacionalidade de algumas ações criminosas; terceiro, solicitar uma resposta conjunta no seio da União Europeia, enquanto a segurança nacional está igualmente comprometida neste domínio, como o Parlamento Europeu considerou reiteradamente; quarto, aperfeiçoar a capacidade de auditoria forense agora exigida pelas normas administrativas e planos públicos, de modo que passe dos conteúdos técnicos à conformação de suportes probatórios inatacáveis nos processos penais.

Relativamente à primeira questão: nos nossos países e no conjunto da União Europeia, verificou-se a enorme dificuldade de comprovar uma repartição de responsabilidades perante a comissão de ilícitos penais mediante um suporte probatório suficiente para prosperar a acusação em sede judicial (Pons Gamon, 2018, p. 119). Se tomarmos os episódios mais impactantes para o funcionamento das empresas em relação aos cibercrimes contra o património, esta já é uma dificuldade notável, mais pelas implicações reputacionais que por verdadeiras dificuldades de averiguação, pois muitas grandes companhias, uma vez resolvida a brecha de segurança dos seus sistemas, preferem enfrentar pagamentos às vítimas do que promover a condenação penal dos criminosos para evitar notícias alarmantes sobre as vulnerabilidades das suas operações no ciberespaço. Contudo, quando se passa dessa esfera para a dos crimes aqui analisados contra a segurança nacional, talvez com a única exceção do

ciberterrorismo (Sánchez Lozano, 2018, Capítulo 2 Retos dos conflitos armados no ciberespaço), assistimos a uma verdadeira incapacidade probatória, seja pelas dificuldades de indagação da autoria ou porque se depara com uma eventual responsabilidade de agentes que possam atuar por conta de Estados terceiros que lhes confiram imunidade. É de lembrar o episódio da ingerência russa através de quase cinco mil *bots* em apoio do desafio secessionista catalão entre 29 de setembro e 19 de outubro de 2017, um dos exemplos enormemente didáticos que serve para compreender a verdadeira natureza do desafio que Espanha e Portugal enfrentam para garantir a cibersegurança nacional.

Agora a relação com a segunda proposta, que tem a ver com as frustrantes restrições impostas à perseguição, investigação e julgamento dos ciberataques contra a segurança nacional quando ocorrem a partir do estrangeiro. Mais uma vez, a ingerência russa exemplifica os problemas que surgem com ações que constituem ilícitos penais segundo o CPE, e que podem ter tratamento diferente noutros Direitos para efeitos da sua perseguição dentro das fronteiras de Estados terceiros. Estes resultam num tratamento prático muito distinto entre os crimes passíveis de procedimento penal, de acordo com as normas do Direito Penal Internacional, e os que não adquiriram um estatuto jurídico tão consolidado, sendo apenas passíveis de procedimento penal nos termos das legislações nacionais.

Nos fatos mais alarmantes falham as previsões construídas pelo Direito Internacional Público para outros cenários, tangíveis ou intangíveis, mas abertos e carentes do anonimato que o carateriza. Basta considerar a doutrina internacionalista, mais que a letra dos acordos internacionais e a escassa jurisprudência disponível sobre os chamados "fatos do Estado" ao considerar um Estado penalmente responsável pelo comportamento de indivíduos que atuam sob instruções, direção ou controlo, uma vez que, neste caso, é mais provável que ocorra perante a inação e a deliberada inibição ou omissão de controlo do Estado do que por mandato expresso.

O Ocidente constatou, através da rastreabilidade tecnológica inequívoca, a origem russa dos ataques às eleições presidenciais americanas de 2016, às eleições presidenciais francesas, às eleições gerais alemãs, à campanha eleitoral do *Brexit* e ao desafio independentista catalão -ingerência russa que foi analisada inclusive no Senado dos Estados Unidos. Todas estas últimas intervenções promovidas pela agência russa *IRA* em 2017. Porém, perante todos e cada um desses eventos a recusa em aceitar responsabilidades do governo russo amparava-se não no seu desconhecimento de tais fatos, mas na impossibilidade de os monitorizar, como ficou evidenciado pela tensa reunião entre os presidentes Putin e Macron em Versalhes. Espanha constatou algo parecido quando o *CERT* Governamental interveio no ciberataque de *ransomware Netwalker,* evitando a encriptação maliciosa das redes de hospitais públicos espanhóis em plena incidência dura da pandemia. Em ambos os casos, saber de onde provêm os ciberataques e poder levar a cabo uma acusação formal, são coisas muito diferentes.

Igual dificuldade de aplicação prática dos princípios do Direito Internacional Público apresenta a definição para o uso da força no ciberespaço dos três conceitos-chave de gravidade, imediatez e intrusão, que resultariam no recurso à força através da resposta de ciberarmas em caso de legítima defesa. Inclusive em casos iminentes, nos mais controversos casos de legítima defesa antecipada que, por definição, no ciberespaço se multiplicariam infinitamente dada a imediatez entre a perpetração do ciberataque e as suas consequências, ao contrário do que acontece no mundo físico que requer movimentos de grupos ou tropas.

Finalmente, entre estas dificuldades de aplicação das disposições do Direito Internacional Público, sobressai a impossibilidade de aplicação *stricto sensu* do princípio da proporcionalidade como complemento ao princípio da necessidade,

uma vez que a assimetria dos meios de comunicação faz parte integrante da guerra híbrida no ciberespaço.

Estes não são os únicos obstáculos processuais. É importante lembrar a complexa determinação da competência jurisdicional territorial penal, em relação aos artigos 14.2 LECr e 7 CPP com grande dificuldade para especificar o local onde o crime foi cometido quando o ataque envolve redes e servidores de diferentes países.

Existe já uma preocupação palpável da União Europeia que veio completar a visão parcial da OTAN (Ganuza Artiles, 2011, pp. 166–169), que contempla a segurança do ponto de vista militar. A integração desse interesse na segurança numa ação conjunta beneficiou de uma rápida mudança de mentalidades. Foi evidente na configuração da Política Externa e de Segurança Comum entre os Tratados de *Maastricht* e de Lisboa que ela necessita de mais reforço depois dos ataques jihadistas sofridos por uma pluralidade de Estados-Membros. Fruto dessa ocupação existem incipientes mecanismos cooperativos (Manrique de Luna Barrios, 2016, p. 388), que estão chamados a intensificar-se, porque as ameaças no ciberespaço estão a ocupar paulatinamente o lugar das ameaças no mundo físico.

É essencial mencionar a conveniência do desenvolvimento da capacidade forense (Caro Lindo, 2015, p. 149) e da auditoria: caminho empreendido desde a técnica até ao Direito, antes de se encerrar esta lista de propostas. Trata-se de aperfeiçoar a capacidade de auditoria forense para permitir imputações ou inculpações com suficiente suporte probatório (Barrio Andrés, 2018; Flores Prada, 2012; Sánchez Magro, 2005, p. 293). Este é atualmente o principal obstáculo que se coloca à perseguição dos crimes com eficácia preventiva, por exemplo. Quando as investigações policiais revelam que a origem do cibercrime está em Portugal ou Espanha, os procedimentos judiciais são os habituais, com uma grande continuidade entre a investigação policial, a instrução, o julgamento e, a eventual condenação. Embora seja sempre desejável uma melhor dotação de meios humanos e materiais, não parece que o escolho se encontre na formação e dotação de unidades especializadas em delitos telemáticos, também contra a segurança, nos corpos policiais integrais. No entanto, ao contrário do que acontece nos cibercrimes contra o património, os crimes cometidos no ciberespaço contra a segurança e a defesa nacionais têm frequentemente origem territorial fora das fronteiras nacionais, em países com pouca cultura e instrumentos obrigatórios de cooperação judiciária internacional.

Embora a Convenção de Budapeste sobre a cibercriminalidade, de 23 de novembro de 2001, ratificada por Espanha em 2010, tenha constituído um marco importante na cooperação internacional em matéria de perseguição penal dos crimes tecnológicos (Díaz Gómez, 2010, p. 170; Jiménez García, 2014, pp. 51–60), está parcialmente desatualizada e, após duas décadas, mostra a sua total inadequação aos níveis de ataque e conetividade atuais. É necessária uma atualização para melhorar a investigação (Asencio Gallego, 2017, pp. 45–49) na fase de instrução que facilita as audiências.

## 6. CONCLUSÕES

Expostas as razões que parecem sustentar uma modificação importante em diversas direções das normas vigentes no que toca à proteção penal da cibersegurança, e mesmo a sua extensão para além dos limites atuais, é oportuno apontar as principais conclusões que constituem estas reflexões, sem necessidade de enumerar novamente as medidas descritas na secção anterior.

A primeira é a constatação do desfasamento normativo devido à obsolescência da regulação pensada para instrumentos tecnológicos menos maduros e invasivos que os atuais. As alterações de teor literal dos artigos do Código Penal obedeciam tradicionalmente a razões dogmáticas, enquanto que aqui parecem ser aconselhadas por razões

de política criminal. Não se trata de procurar uma maior punição, mas uma melhor definição dos elementos objetivos do tipo penal, especificando condutas dolosas com pluralidade de intervenientes e sucessão de atos de execução. No que diz respeito à normativa própria do âmbito do Direito Digital, aprecia-se uma maior atualização constante, pelo que se trata unicamente de incluir mecanismos de antecipação à produção efetiva de danos graves à segurança nacional, o que abre um novo debate de política criminal em relação à ampliação, não tanto das penas aplicadas nas condenações, mas à possibilidade de aplicação de medidas de segurança para remover preventivamente o perigo abstrato de ciberataque contra serviços básicos da Segurança Nacional mediante a interdição de atividades informáticas, além das previsões de aplicação do artigo 100 CPP para arguidos não condenados sem chegar às previsões do artigo 199.1.b do Código do Processo Penal.

A segunda é a necessidade de evitar uma compartimentação perniciosa como a atual entre ilícitos penais e ilícitos administrativos, em que os primeiros aparecem diluídos e os segundos revelam-se incapazes de conter os ciberataques que passam de riscos a vulnerações efetivas da segurança nacional. Este objetivo só será alcançado através de soluções jurídicas interdisciplinares que pretendam uma maior eficácia da persecução penal dos delitos e da investigação policial nos casos mais afetados pela extraterritorialidade e o anonimato proporcionado pelo ciberespaço. Para isso, devem intensificar-se as pontes entre a perspetiva processual penal e o Direito Penal.

A terceira é a necessidade de projetar nas próximas mudanças das reformas legislativas a amplitude normativa das Lei de Segurança Interna portuguesa e Lei de Segurança Nacional espanhola, que nestes momentos parecem desacopladas da proteção penal. A sua maior flexibilidade para acomodar estas abordagens jurídicas interdisciplinares pode informar de forma eficiente reformas legislativas simultâneas que, no futuro imediato, agilizem os mecanismos de resiliência e recuperação face a ataques cibernéticos graves à segurança cibernética nacional no que diz respeito aos Códigos Penais e do Processo Penal. Chama-se a atenção para a necessidade de fazê-lo nessa ordem, uma vez que abordar parcialmente reformas legislativas incompletas de regras processuais sem resolver previamente o impacto das ações típicas sobre a autoria é um exercício abocado à frustração.

A quarta é a conveniência em implementar algumas das reformas mais urgentes propostas neste artigo dentro de um prazo razoável e curto, dentro das atuais legislaturas estatais, aproveitando a necessidade de transpor as modificações na norma comunitária que possam afetar as ferramentas utilizadas no ciberespaço e que têm implicações de cibersegurança, que inevitavelmente afetam a Segurança Nacional. Felizmente, algumas das inovações regulamentares comunitárias foram implementadas através de regulamentos de aplicação direta em todos os Estados-membros da UE, e não através de diretivas que exigem uma transposição positiva. No entanto, é também verdade que mesmo o conteúdo dos regulamentos precisa de ser incorporado nas leis nacionais, como já aconteceu com a proteção de dados pessoais, de forma global e, com *blockchain* e inteligência artificial de forma ainda parcial.

A principal necessidade é especificar a conduta dolosa punível nos elementos objetivos dos tipos através de uma reforma da sua literalidade. Delimitar a punição pelas ações e não pelo resultado é a melhor forma de evitar ter de alterar os artigos referentes à autoria e comparticipação, através de uma descrição detalhada da conduta dolosa diferente da eventual culpa dos prestadores de serviços digitais.

Os mecanismos sancionatórios previstos no Direito Digital são absolutamente insuficientes face ao aumento de casos relativamente graves de ataques no ciberespaço contra redes, dados e serviços policiais e militares, intensificados pela atual situação de tensão internacional. O Direito Penal deve mostrar a sua capacidade protetora, com um delicado equilíbrio entre interesses estratégicos em jogo e a proteção dos

direitos constitucionais fundamentais dos cidadãos portugueses e espanhóis, sem sucumbir ao populismo punitivo, mas oferecendo soluções eficazes às tentativas de tensionar a convivência social por meio de engenharia social deliberada para provocar situações de desproteção, além da mera desinformação massiva que responde às estratégias desestabilizadoras de atores estatais.

## 7. BIBLIOGRAFIA


Aires de Sousa, S. (2020). Não fui eu, foi a máquina": Teoria do crime, responsabilidade e inteligência artificial. Em A. Miranda Rodrigues (Ed.), *A Inteligência Artificial no Direito Penal* (pp. 59–94). Almedina.

Alcantarilla, J. (2016). «Big Data» en los departamentos de seguridad, una oportunidad para un nuevo modelo. *Seguritecnia*, *434*, 48–49.

Aldana Montes, J. F., García Nieto, J. M., Gonzalvez, J. C., e Navas Delgado, I. (2018). *Big data: Seguridad y gobernanza*. García Maroto Editores.

Alonso García, J. (2015). *Derecho penal y redes sociales*. Thomson Reuters Aranzadi.

Álvarez Rodríguez, I. (2019). Constitución y Derecho del Ciberespacio. Em C. Mallada Fernández (Ed.), *Nuevos retos de la ciberseguridad en un contexto cambiante* (pp. 21–46). Aranzadi Thomson Reuters.

Arias Holguín, D. P. (2018). Contexto, interdisciplinariedad y dogmática penal. Em *Liber amicorum: Estudios jurídicos en homenaje al profesor doctor Juan Ma. Terradillos Basoco* (pp. 49–62). Tirant lo Blanch.

Arteaga Martín, F. (2019). Contexto estratégico de la inteligencia artificial. Em *La inteligencia artificial, aplicada a la defensa* (pp. 153–172).

Asencio Gallego, J. M. (2017). Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia. Em *Justicia penal y nuevas formas de delincuencia* (pp. 44–67). Tirant lo Blanch.

Barcelar Gouveia, J. (2022). *Defesa nacional e forças armadas: Uma perspectiva no direito militar da segurança em Estado constitucional democrático*. Almedina.

Barrio Andrés, M. (2018). *Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos*. Wolters Kluwer.

Caro Lindo, A. (2015). Reto en ciberseguridad: Análisis forense de discos. Em *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015. I JNIC2015* (pp. 148–155). Área de Publicaciones Universidad de León.

Carrillo Ruiz, J. A., Marco de Lucas, J., Dueñas López, J. C., Cases Vega, F., Cristino Fernández, J., González Muñoz De Morales, G., e Pereda Laredo, L. F. (2013). Big data en los entornos de defensa y seguridad. *Pre-bie3*, *6*.

Cubeiro Cabello, E. (2020). Inteligencia artificial para la seguridad y defensa del ciberespacio. Em *Usos militares de la inteligencia artificial, la automatización y la robótica* (pp. 97–130).

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR*, *8*, 169–203.

Fernandes Godinho, I., Flores, C., e Castro Marques, N. (2020). Consultation on The White Paper on Artificial Intelligence – A European Approach. *ULP Law Review*, *14*(1), 157–167.

Fernández Bermejo, D., e Martínez Atienza, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Aranzadi Thomson Reuters.

Flores Prada, I. (2012). *Criminalidad informática: (Aspectos sustantivos y procesales)*. Tirant lo Blanch.

Fuente Chacón, J. C. de la. (2019). La inteligencia artificial y su aplicación en el mundo militar. Em *La inteligencia artificial, aplicada a la defensa* (pp. 69–98).

Ganuza Artiles, N. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia*, *149*, 165–214.

Gómez de Ágreda, Á. (2021). Ciberseguridad en un mundo hiperconectado. Em D. Canals i Ametller (Ed.), *Ciberseguridad. Un nuevo reto para el Estado y los gobiernos locales* (pp. 29–62). Wolters Kluwer.

Goncalves, O. O., e Mascarello Luciani, D. C. (2023). A utilização de análises preditivas na era da hiperconectividade: O futuro do mercado com a internet das coisas (IoT). *Ano 9*, *1*, 1123–1146.

González Hurtado, J. A. (2014). Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: La seguridad en los sistemas de información. *La ley penal: revista de derecho penal, procesal y penitenciario*, *107*, 4.

González Rus, J. J. (2006). Los ilícitos en la red (I): Hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes. Em *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales.* (pp. 241–271). Comares.

Gorra, D. G. (2014). ¿Los jueces crean derecho cuando "definen" los tipos penales abiertos? *Revista de Derecho Penal y Criminología*, 7, 199–206.

Gutbrod, M. (2020). Digital transformation in economy and law. *Digital Law Journal*, *1*(1), 12–23.

Gutiérrez Espada, C. (2020). ¿Existe (ya) un derecho aplicable a las actividades en el ciberespacio? Em M. J. Cervell Hortal (Ed.), *Nuevas tecnologías en el uso de la fuerza: Drones, armas autónomas y ciberespacio* (pp. 225–248). Thomson Reuters Aranzadi.

Hörnle, J. (2020). *Internet Jurisdiction Law and Practice*. Oxford University Press.

Jiménez García, F. (2014). La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa. Em *La protección y seguridad de la persona en internet: Aspectos sociales y jurídicos* (pp. 49–79). Madrid : Reus, 2014.

Lemos, M., e Costa, M. J. (2022). Inteligência artificial e Direito da Guerra: Reflexões sobre as armas autónomas mortíferas. Em A. Miranda Rodrigues (Ed.), *A Inteligência Artificial no Direito Penal: Vol. II* (pp. 91–124). Almedina.

Malhado, R. (2017). Big Data y sistemas cognitivos están cambiando el paradigma de seguridad. *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, *78*, 42–44.

Manrique de Luna Barrios, A. (2016). El rol de la Unión Europea en el ámbito de la paz y de la seguridad regional e internacional. Em S. de Tomás Morales (Ed.), *Retos del Derecho ante las nuevas amenazas* (pp. 387–396). Dykinson.

Márquez Díaz, J. E. (2017). Armas cibernéticas. Malware inteligente para ataques dirigidos. *Revista Ingenierías USBMed*, *8*(2), 48–57.

Meirelles Magalhães, F. de A. (2021). Smart contracts: O jurista como programador. Em M. R. Guimarães, R. Teixeira Pedro, e M. R. Redinha (Eds.), *Direito Digital* (pp. 5–72). Universidade do Porto.

Miceli, J. E., Orsi, O. G., e Rodríguez García, N. (2017). *Análisis de redes sociales y sistema penal*. Tirant lo Blanch.

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Moret Millás, V. (2020). Blockchain and National Security. *Revista de privacidad y derecho digital*, *5*(18), 97–128.

Navarro Bonilla, D. (2014). Espionaje, seguridad nacional y relaciones internacionales. *Colección de estudios internacionales*, *14*, 1–45.

Navarro, M. (2016). La seguridad se convierte en el principal reto de Big Data. *Byte España*, *238*, 8–9.

Neiva, L. (2021). Big data e vigilância policial: Desafíos éticos, legais e sociais. Em *Crime e tecnologia. Desafos culturais e políticos para a Europa* (pp. 65–90). Afrontamento.

Periago Morant, J. (2019). TICS y Redes Sociales en derecho penal: Pensamiento analítico. Em *IN-RED 2019: V Congreso de Innovación Educativa y Docencia en Red* (pp. 488–501).

Picotti, L. (2019). Ciberespacio y Derecho penal. Em G. Basso (Ed.), *Libro homenaje al profesor Dr. Agustín Jorge Barreiro* (Vol. 2, pp. 1191–1204). Servicio de Publicaciones de la Universidad Autónoma de Madrid.

Pons Gamon, V. (2018). *Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*. UNED.

Requena Jiménez, A. (2017). Blockchain como disrupción para aplicaciones de seguridad. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, *26*(127), 114–116.

Romeo Casabona, C. M. (2022). La atribución de responsabilidad penal por los hechos cometidos por sistemas autónomos inteligentes, robótica y tecnologías conexas. ULP Law Review, 16(1), 7–16.

Sánchez Lozano, M. L. (2018). *Los retos del derecho internacional humanitario para los conflictos armados en el ciberespacio*. Grupo Editorial Ibáñez.

Sánchez Magro, A. (2005). El ciberdelito y sus implicaciones procesales. Em P. L. García Mexía (Ed.), *Principios de derecho de internet* (pp. 293–324). Tirant lo Blanch.

Schwalbach, J. G. (2021). *Direito Digital*. Almedina.

Serrano Ferrer, M. P. (2016). *El reflejo de las nuevas tecnologías en el derecho penal y otros destellos*. Aranzadi Thomson Reuters.

Sidorenko, E., e von Arx, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. *Digital Law Journal*, *1*(1), 24–38.

Silva Rodrigues, B. (2009). *Direito Penal Informático-Digital*. Coimbra Editora.

Singer, P. W. (2015). Ciberarmas y carreras de armamentos: Un análisis. *Vanguardia dossier*, *54*, 42–47.

Suñé Llinas, E. (2007). Del derecho de la informática al derecho del ciberespacio y a la constitución del ciberespacio. *Estudios jurídicos*, *2007*.

Torío López, Á. (1995). Tipicidad. Referencia a la teoría de los tipos abiertos. Em J. Jiménez Villarejo (Ed.), *Vinculación del juez a la ley penal* (pp. 7–34). Consejo General del Poder Judicial.

Valls Estefanell, M. (2018). La inteligencia artificial y su encaje en las Estrategias de Seguridad Nacional. *bie3: Boletín IEEE*, *12*, 472–485.

Vilela, A. (2022). Is the Legislator of Sanctionatory Law Attentive to Criminal Policy? *US-China Law Review*, *2*, 92–98.