# ALGUMAS CONSIDERAÇÕES POLÍTICO-CRIMINAIS A PROPÓSITO DA CIBERSEGURANÇA

Pedro Jacob Morais[1]
https://doi.org/10.21814/uminho.ed.151.14

## 1. Considerações introdutórias

O direito penal encontra-se matricialmente marcado pelo signo da contingência, pela circunstância sempre mutável no dinamismo do binómio espaço-tempo. Assim sendo, os desafios jurídico-penais apresentam-se sempre históricos, no preciso sentido de que o direito penal assenta num concreto *hic et nunc*. Neste sentido, a circunstância espácio-temporal que circunda e secunda o fenómeno criminal demanda desafios jurídico-penais diversos, realizados, ou seja, que contactem com a realidade e que, nesse contacto, se transformem materialmente num dos seus elementos constitutivos.

Não necessitamos de recuar a Liszt e aos alvores da "ciência conjunta do direito penal"[2] para compreendermos com cada vez maior agudeza que o fenómeno criminal demanda um tratamento sistémico. Um tratamento

[1] Professor Auxiliar da Escola de Direito da Universidade do Minho.

[2] Para a compreensão o conceito original, cfr. LISZT, Franz von - *Strafrechtliche Aufsätze und Vorträge*. Berlin: Walter Gruyter & Co., 1970, pág. 290 e ss [em especial, pág. 283 e ss].

sistémico que, sob pena de exiguidade problemática, não deve ser reduzido à estreiteza da amurada da dogmática penal. Destarte, o direito penal perfila-se como parte integrante de um sistema mais complexo e amplo de justiça. No seio deste sistema, o direito penal compreende um cômputo ou, melhor, representa uma unidade sistémica substantivo-adjectiva. Uma unidade sistémica capaz de exponenciar a comunicação e a harmonização de soluções entre o direito penal e o direito processual penal. Ademais, no sistema de justiça em estudo, a criminologia surge como ciência preparadora do direito penal. No seu arquipélago de interdisciplinaridade[3], a criminologia não se limita a explicar mecânico-causalmente o surgimento do fenómeno criminal, mas valida as opções normativas e acompanha a decisão judicativa[4]. Por fim, não devemos perder de vista a política criminal como parte essencial da equação da justiça penal[5]. Política criminal que actua como o vector-guia do *ius puniendi* estatal, linha de fuga a quadrar as principais opções jurídico-penais do Estado. Claro que as concretas opções político-criminais devem encontrar-se orientadas e balizadas pelos resultados dos estudos do direto penal substantivo e adjectivo, bem como pela investigação criminológica.

O direito penal substantivo e adjectivo, a criminologia e a política criminal encetam um conjunto de relações de mútua perturbação ou, dito de modo diverso, de mútuo contributo e aperfeiçoamento a que damos o nome de sistema global de justiça penal[6]. Note-se que não nos referimos à supramencionada "ciência conjunta do direito penal", visto que agora, ao contrário de antanho, a dogmática penal não tem de se soerguer num amuralhamento de marfim, avesso a influências externas. A dogmática penal já não se

---

[3] A incidir na ideia da interdisciplinaridade, ver o conjunto de textos organizados em AGRA, Cândido da – *A Criminologia: Um arquipélago inderdisciplinar*. Porto: U.Porto, 2012.

[4] Sobre a relação entre a criminologia, o direito penal e a política criminal, ver DIAS, Jorge de Figueiredo; ANDRADE, Manuel da Costa - *Criminologia: O homem delinquente e a sociedade criminógena*. Coimbra: Coimbra Editora, 1992, pp. 96 e ss.

[5] De acordo com a lição de DIAS, Jorge de Figueiredo - *Direito Penal: Parte Geral. Tomo I: As Questões Fundamentais. A Doutrina Geral do Crime*. Coimbra: Gestlegal, 2019, pp. 38 e 39, "[a] política criminal, de ciência simplesmente competente para as tarefas da reforma penal, cujas proposições, por conseguinte, não podiam ser levadas em conta senão no plano do *iure constituendo*, torna-se em ciência competente para, em último termo, definir os limites da punibilidade".

[6] A propor e a desenvolver o conceito de "sistema global de justiça penal", ver MONTE, Mário Ferreira, *Apontamentos de Direito Penal*. I: Fundamentos, Teoria da Lei Penal, 2021 (exemplar policopiado gentilmente cedido pelo Autor), pp. 55 e ss, e idem, "Da realização Integral do Direito Penal". In Dias, Jorge de Figueiredo, [et al.], Estudos de Homenagem ao Prof. Doutor António Castanheira Neves. Coimbra: Coimbra Editora, 2008. Vol. 3, pp. 752 e ss.

perspectiva como a "barreira insuperável da política criminal"[7]. Pelo exposto, a contemporaneidade demanda uma abordagem conjunta das diversas ciências criminais na resolução do fenómeno criminal. Uma abordagem não hierárquica ou pré-concebida, uma abordagem que não é coutada dos juristas, dos criminólogos ou dos operadores políticos. Uma abordagem que reconhece a premência social dos desafios colocados pela criminalidade, nas suas diversas declinações e, para o que nos ocupa, na sua dimensão cibernética.

## 2. Aproximação à cibersegurança e à cibercriminalidade

Antes de nos adentrarmos no tratamento político-criminal da cibersegurança e da cibercriminalidade, tentemos uma aproximação aos conceitos em estudo. Os desafios cibernéticos convocam a separação entre o mundo físico e o mundo digital, como se de duas linguagens ou de dois universos incompatível ou refractários se tratassem. Como se o mundo digital estivesse firmado num tempo e num espaço próprios que o impedissem de comunicar com o mundo físico. Um tempo digital, diacrónico, encerrado sob si próprio e aparentemente diverso do tempo analógico que marca o sincronismo espácio-temporal do mundo dito físico[8].

Em termos semiológicos, o mundo físico e o mundo digital parecem firmar uma oposição insanável, como se o mundo digital não fosse real, como se fosse um mero simulacro ou simulação[9]. Como se o mundo digital não interferisse ou não afectasse o mundo dito real. Como se pudéssemos distinguir um mundo autêntico e um sucedâneo de mundo. Notemos que a "busca pela autenticidade", esta procura pelo tecido da realidade que ocupa a reflexão em torno dos desafios digitais possui raízes filosóficas muito profundas. Pensemos, a título de exemplo, na Alegoria da Caverna de Platão e na distinção entre o mundo das ideias e o mundo dos sentidos[10], na clivagem

[7] A analisar detidamente esta "barreira insuperável", ver MUÑOZ CONDE, Francisco – "La herancia de Franz von Liszt". Revista Penal México. nº 2 (2011), p. 58 e ss.

[8] Sobre o tempo analógico e o tempo digital, cfr. LANDES, David S . - *A Revolução no Tempo.* Lisboa: Gradiva, 2009.

[9] A propósito dos conceitos de simulação e simulacro, ver BAUDRILLARD, Jean – *Simulacros e Simulação.* Lisboa: Relógio D'Água, 1991, p. 11 e ss.

[10] Cfr. PLATÃO – *A República*. Porto: Fundação Calouste Gulbenkian, 2008, p. 315 e ss [514a e ss].

agostiniana entre a cidade de Deus e a cidade dos homens, na contraposição kantiana insanável entre número e fenómeno[11], ou na clareia heideggeriana entre o *sein* e o *dasein*[12]. Esta permanente preocupação acompanhante da filosofia influenciou claramente diversas expressões artísticas populares através de lugares-comuns. Pensemos, como mero exemplo, em obras cinematográficas como "Mundo no Arame" (1973), "Ghost in the Shell" (1995) ou "Matrix" (1999) e na fractura entre o mundo físico e o mundo digital que convocam. Uma fractura que não deixa de representar, em jeito de paradoxo, uma inevitável imbricação ou interferência mútua que, a seu tempo, abordaremos. Nestas obras cinematográficas, o protagonista invariavelmente desperta para a realidade, transita do sonho para a vigília apercebe-se de que aquilo que julgava ser a realidade não passava de uma simulação ou de um simulacro.

## 3. Ameaças cibernéticas e respectivos corolários

De volta à realidade contingente, os ordenamentos jurídicos, independentemente da sua conformação, têm vindo a ser assolados por diversas ameaças cibernéticas. Refira-se os pedidos de resgate ("ransomware") a pessoas singulares e colectivas, o acesso a dados bancários e a servidores informáticos ou os problemas de segurança convocados pela "internet das coisas"[13]. Dizíamos que as ameaças cibernéticas atingem os diversos ordenamentos jurídicos, independentemente da sua conformação, na medida em que o desenvolvimento do mundo digital está intimamente relacionado com a globalização ou com o processo globalizante em curso, se preferirmos. Nesta redução exponencial de distâncias ou subversão da relação de proporcionalidade directa entre o espaço e o tempo que caracteriza a globalização, o cibermundo compreende um *locus* sem fronteiras, dando clara expressão à

[11] Vide KANT, Immanuel - *Fundamentação da Metafísica dos Costumes*. Lisboa: Edições 70, 2008, p. 115 e ss.

[12] Cfr. HEIDEGGER, Martin - *Ser y Tiempo*. Editorial Trotta, 2018, p. 63 e ss.

[13] Numa aproximação ao conceito de "internet das coisas", ver FACHANA, João – *Que Papel Para o Consentimento na Sociedade em Rede?* In Neto, Luísa; Ribeiro, Fernanda – *Direito e Informação na Sociedade em Rede: Atas.* Porto: Faculdade de Direito e Faculdade de Letras da Universidade do Porto, 2016, p. 100 e ss.

ubiquidade do risco e da incerteza[14], à modernidade líquida[15], à sociedade da transparência[16], entre outros conceitos equivalentes.

Ainda que o campo lexical da sociedade do risco não corresponda a um cenário distópico, encontrando-se umbilicalmente ligado ao desenvolvimento humano por via da exponenciação da mobilidade humana, do tráfego de bens e da disponibilização de serviços, não podemos deixar de notar uma dimensão menos solar e mais lunar do entrechoque entre globalização e o cibermundo. Entrechoque e relação conatural, na medida em que o desenvolvimento do mundo digital se encontra intimamente relacionado com o desenvolvimento e expansão da globalização[17]. Neste concreto sentido, o cibermundo ou ciberespaço, tal como o conhecemos hoje, representa um dos corolários da globalização, na medida em que constitui um incontornável coadjuvante das deslocações humanas e de bens, tal como da disponibilização de serviços. Todavia, não podemos olvidar que o mundo digital constitui um *locus* sem fronteiras, expressando com clareza a ubiquidade do risco e da incerteza, e que tem soerguido zonas sombrias, de difícil acesso e propiciadoras de criminalidade. Bem observado, e à semelhança do que ocorre no mundo físico, a globalização tem permitido o surgimento daquilo que Bauman designa como "zona fronteiriça global"[18] ou, se preferirmos a designação de Agamben[19],

---

[14] Falamos da redução exponencial de distâncias comummente designada como globalização (para uma compreensão aprofundada do fenómeno em causa, ver BECK, Ulrich – *What is Globalization?* Malden: Polity Press, 2009, pp. 30 e ss.) e das profundas consequências sociais que provocou, quer em termos de percepção do espaço na sua vertente geopolítica, quer em termos de relacionamento intersubjetivo (a servir-se da expressão "sociedade do risco relacional", CASTALDO, Andrea R. – *Welches Strafrecht für das neue Jahrtausend?* In Schünemann, Bernd – Festschrift für Claus Roxin zum 70. Geburtstag am 15. Mai 2001. Berlin: Walter de Gruyter, 2001. p.g. 110; sobre a ubiquidade do risco, PAWLIK, Michael – *Der rechtfertigende Defensivnotstand im System der Notrechte*. GA. n. 1 (2003), p. 21). Redução de distâncias que assume não raras vezes a feição do confronto entre homogeneidade e heterogeneidade, uniformização e diversificação, enfim, a globalização niveladora e a globalização que respeita as identidades locais, também designada como "glocalização" (ver ROBERTSON, Roland – *Glocalization: Time-Space and Homogeneity-Heterogeneity*. In Featherstone, Mike, [et al.] – Global Modernities. London: Sage, 1995, pp. 25 a 42).

[15] A descrever a transi..o da modernidade s.lida para a modernidade l.quida, *vide* BAUMAN, Zygmunt — *Confiança e Medo na Cidade*. Lisboa: Relógio D'Água, 2006. p. 24. Para uma análise mais aprofundada deste tópico, consultar BAUMAN, Zygmunt – *Liquid Times: Living in an Age of Uncertainty*. Cambridge: Polity, 2007, pp. 5 e ss.

[16] Tal como desenvolvido em HAN, Byung-Chul – *A Sociedade da Transparência*. Lisboa: Relógio D'Água, 2014, em claro corte com o referente imunitário desimplicado em ESPOSITO, Roberto – *Immunitas: Protección y negación de la vida*. Madrid: Amorrortu, 2009.

[17] Em sentido semelhante, mas a traçar um elo entre a globalização e a "evolução da criminalidade organizada", ver CABRAL, José Santos – *Uma Incursão Pela Polícia*. Coimbra: Almedina, 2007, p. 13 e ss.

[18] Cfr. BAUMAN, Zygmunt – Sociedade Sitiada. Lisboa: Instituto Piaget, 2010, p. 112 e ss.

[19] *Vide* AGAMBEN, Giorgio – *O Poder Soberano e a Vida Nua: Homo Sacer*. Lisboa: Editorial Presença, 1998, pp. 115 e ss.

assistimos ao (re)surgimento dos "lager", locais livres da pesquisa estatal, verdadeiros não-Estados ou contra-Estados avessos à normação jurídica[20].

O mundo digital, pela extensão difícil de abarcar, pelo estranhamento que ainda provoca junto das comunidades que compõem a sociedade, e pelo célere desenvolvimento que parece incompatível com a estabilidade normativa que a certeza e a segurança jurídica demandam, surge não raras vezes como um espaço de anomia. Pensemos, como frontão desta anomia, no pungente exemplo na "deep web" que, podendo servir como uma ferramenta jornalística imprescindível perante regimes autoritários ou totalitários, convoca igualmente preocupações criminais profundas[21]. Convoca-as na medida em que a "deep weeb" constitui exactamente uma zona fronteiriça global, porquanto se perfila refractária não apenas à normação estatal mas também à própria consciência axiológica da sociedade, uma vez que não permite a mediação normativa que possibilita a cidadania (eu-norma-outro)[22].

Imbuídos pela perplexidade despontada pela "internet" profunda, formulemos algumas questões para reflexão:

- Constituirá o mundo digital ou, melhor, parte do mundo digital o sucedâneo pós-moderno do oeste selvagem? Terra de ninguém, inexplorada ou, em larga medida, por explorar? Ou, olhando o problema sob outro prisma, uma variação distópica dos cenários literários e cinematográficos ditos pós-apocalípticos[23]?
- Compreenderá um *locus* ou diversos *loci* anómicos, avessos à normação jurídica?

[20] A propósito dos conceitos de "Estado", "não-Estado" e "contra-Estado", ver MORAIS, Pedro Jacob – *O Crime e a Cidade - A(s) arquitectura(s) da prevenção*. In Monte, Mário Ferreira*, [et al.]*- Prevenção, Policiamento e Segurança: Implicações nos Direitos Humanos. Braga: EDUM/JusGov, 2022, p. 34 e 35.

[21] A enquadrar a "deep web", cfr. SUI, Daniele; Caverlee, James; Sui, Daniel- "The Deep Web and the Darknet: A Look Inside the Internet's Massive Back Box". Ohio State Public Law Working Paper. nº 314 (2015), pp. 5 e ss.

[22] Sobre os trinómio "eu-norma-outro" e "eu-anomia-outro", *vide* MORAIS, Pedro Jacob – *Breve Apontamento Sobre a Violência e o Poder: Do Estado-corpo ao Estado-máquin*a. In Leite, André Lamas*, [et al.]* – O Sentir do Direito. Estudos em Homenagem ao Professor José Tavares de Sousa. Lisboa: AAFDL, 2022, pp. 275 e 276.

[23] Ainda que a origem do género cinematográfico comummente designado como pós-apocalíptico possa recuar aos alvores da história do cinema pensemos, pelo reconhecimento popular que granjeia, no filme "Mad Max" (1979), por confrontar o espectador com um mundo onde a anomia substituiu a normação jurídica e onde o binómio segurança-liberdade soçobrou perante a ameaça constante.

- Até onde estamos dispostos a ir, em termos de limitação de direitos, liberdades e garantias para dominar ou conquistar o ciberespaço?

Aqui chegados, a cibersegurança e, para sermos mais precisos, a cibercriminalidade convoca desafios assinaláveis ao sistema global de justiça penal. Convoca-os pela diversidade de tipos legais de que se pode revestir, pela inadaptação de alguns tipos legais originalmente pensados para o mundo físico, pela necessidade de actualização normativa do sistema jurídico por via de novas tipologias criminais. Mais convoca desafios assinaláveis, na medida em que começa a surgir, não apenas a preocupação, mas uma verdadeira percepção de que a cibercriminalidade se encontra intimamente relacionada com fenómenos tão prementes como a criminalidade violenta, a criminalidade organizada e o terrorismo[24]. Fenómenos estes que conhecem novas declinações no mundo digital e que possuem uma particular potencialidade erosiva das estruturas do Estado e da sociedade. A cibercriminalidade configura um assinalável obstáculo para as sociedades abertas e pluralistas, bem como para os Estados de direito em sentido material. Assim ocorre, por um lado, devido à vulneração indiscriminada ou à vulnerabilidade generalizada dos cidadãos perante a ciber-ameaça e, por outro lado, devido aos perigos acrescidos que se vêm avolumando em torno das estruturas, ou infra-estruturas essenciais dos Estados, como sejam os sistemas de justiça, de saúde, de educação, de segurança rodoviária, aeronáutica, marítima, entre outros. De volta à semiologia, podemos intuir que a existência e eventual expansão dos espaços de anomia no mundo digital poderá metastizar ou contaminar a normação jurídica e, como corolário necessário, perigar o Estado, mais especificamente os seus subsistemas, bem como outras estruturas essenciais da sociedade. Em suma, a anomia da zona fronteiriça global cibernética poderá inquinar a normação estatal num duplo sentido. Em primeiro lugar, por macular a paz jurídica ou, dito de outra forma, por fomentar a percepção comunitária de que os tipos legais são letra morta na carência do reforço contrafáctico das expectativas comunitárias na vigência da norma violada. Como se o tipo

[24] Numa análise das diversas declinações do ciberterrorismo, ver FREITAS, Pedro Miguel – "Ciberterrorismo e a Lei de Combate ao Terrorismo". Nação e Defesa. nº 161 (2022), pp. 116 e ss.

legal violado passasse a ser lei sem vigência enquadrável no grafema força-de-lei de Agamben[25]. Por outro lado, porque a força centrífuga da anomia pode originar como reacção uma força centrífuga normativa igualmente perniciosa. Referimo-nos à vertigem e à tentação da hipercriminalização para fazer frente às ameaças cibernéticas, o apelo do neopunitivismo como perigosa panaceia para o fenómeno criminal, perigosa porque erigida à custa dos direitos, liberdades e garantias dos cidadãos. Notemos que, qualquer que seja a via trilhada, topamos sempre com o binómio segurança-liberdade, a saber. A expansão da anomia conduz à rarefacção da segurança e à reificação de uma liberdade que mais não é do que *liberum arbitrium indifferentiæ*. Por sua vez, a exponenciação do punitivismo reduz a liberdade em favor de uma segurança puramente asséptica. Uma segurança que vota a sociedade ao imobilismo de formol.

## 4. A cibersegurança no contexto internacional e europeu

Antes de encetarmos um plano panorâmico a propósito da cibersegurança no contexto português e europeu, urge questionar se realmente existe uma diferença significativa entre cibersegurança e segurança, mais especificamente entre a cibersegurança e a segurança interna. Certamente serão elencáveis especificidades que enformam a cibersegurança, especificidades que contendem com as suas idiossincrasias técnicas e com a concreta conformação do mundo digital. Contudo, a cibersegurança não deixa de contender com a prevenção criminal, na sua dimensão pré e pós-delitiva; a ordem e a tranquilidade públicas; o normal funcionamento do Estado, mais especificamente dos subsistemas essenciais que o compõem; e ainda o normal funcionamento de setores privados estratégicos como a banca, a aeronáutica ou a distribuição energética. Em suma, a cibersegurança contende com a estabilidade comunitária da sociedade ou, dito de modo mais claro, com a erosão das normas comuns, com a mediação normativa que une os membros da sociedade.

[25] Cfr. AGAMBEN, Giorgio – *Estado de Excepção*. Lisboa: Edições 70, 2010, pp. 55 e ss.

Aproximando-nos do ordenamento jurídico português, ainda que a relação de identidade entre a segurança e a cibersegurança não surja expressamente referida, esta última enquadra-se perfeitamente na Lei de Segurança Interna (Lei 53/2008, de 29 de Agosto). Atentemos à definição de segurança interna presente no artº 1º, nº 1 deste diploma:

> "A segurança interna é a actividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática".

Como é bom de ver, a definição de segurança interna coloca o enfoque na atribuição fundamental do Estado que se consubstancia na prevenção criminal em sentido amplo. Em sentido amplo, na medida em que não atende apenas à reacção jurídica pós-delitiva, mas manifesta igualmente preocupação com a prevenção pré-delitiva, numa clara tomada de consciência de que a insegurança afecta, não apenas os cidadãos individualmente considerados, mas também o "normal funcionamento das instituições democráticas". A segurança interna consiste, em jeito de súmula, na atribuição essencial do Estado de estabilizar e manter o *status quo* comunitário ou, dito de forma diversa, da consecução e manutenção da paz jurídica.

Aqui chegados, a cibersegurança constitui uma das declinações da segurança interna, pelo que deve figurar entre as preocupações político-criminais mais prementes da contemporaneidade jurídica. Contudo, as questões de segurança que rodeiam o mundo digital que, como referimos anteriormente, se perfila conaturalmente ausente e avesso a fronteiras, não se esgota no panorama interno. Ao invés, a cibersegurança tem despertado um intenso labor normativo, não apenas transnacional e europeu, mas também internacional. Em bom rigor, a complexidade dos desafios colocados pelas ameaças cibernéticas apenas pode ser reduzida por via de uma acção complexiva e concertada inter-estatal. Bem se compreende que um problema global dificilmente possa ser resolvido através de soluções meramente locais.

Recuando ao dealbar do milénio, encontramos uma das principais pedras de toque da normação em torno da cibercriminalidade. Referimo-nos à Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001. Ainda que a análise aprofundada da Convenção de Budapeste escape ao objecto do presente estudo, não podemos deixar de referir as preocupações candentes que enformam o diploma[26]. Logo no preâmbulo encontramos o reconhecimento da necessidade de cooperação internacional, tendo em conta que a cibercriminalidade não se reconduz apenas às fronteiras estatais, mas deve convocar o labor da comunidade internacional. Note-se que, mais de uma preocupação genérica, o preâmbulo da Convenção de Budapeste refere expressamente a necessidade da uma política criminal comum entre os diversos Estados, dístico da conformação não local ou estatal das questões em análise. Dístico, diga-se, da relação umbilical entre a globalização e a digitalização, relação esta que se traduz em novas ameaças criminais e desafios criminógenos advindos da utilização de novas tecnologias. Para além da cooperação internacional, a Convenção de Istambul sublinha a importância da "cooperação entre os Estados e a indústria privada no combate ao cibercrime", questão cada vez mais destacada, tomando em linha de conta os conhecimentos e a relevância social da indústria. Por fim, refira-se ainda a preocupação do diploma em torno da protecção dos direitos fundamentais dos cidadãos, com particular incidência no direito à liberdade de opinião e de expressão.

Também a União Europeia tem demonstrado preocupação com o problema da cibersegurança e da cibercriminalidade. Preocupação notória, logo em 2004, com a criação da Agência Europeia para a Cibersegurança (ENISA)[27], entidade administrativa independente[28] que apresenta como escopo garantir um elevado nível de cibersegurança na União Europeia.

---

[26] Para um enquadramento da Convenção de Istambul, cfr. VENÂNCIO, Pedro Dias – *Lições de Direito do Cibercrime. E da tutela de dados pessoais.* Coimbra: Editora d'Ideias, 2022, pp. 52 e ss.

[27] A ENISA foi criada pelo Regulamento (CE) 460/2004 do Parlamento e do Conselho, de 10 de Março de 2004. Posteriormente o seu mandato foi sucessivamente ampliado pelos Regulamentos (CE) 1007/2008, 580/2011 e pelo Regulamento (EU) 526/2013.

[28] As entidades administrativas independentes surgem "como resposta à necessidade de neutralizar certos setores de intervenção pública. (...)." Para mais desenvolvimentos, consultar B*ARROS*, Rita Ribeiro de, Tese Mestrado: *As Agências Europeias no Direito Administrativo Europeu*, EDUM, 2014, pp. 24 e ss.

Outro marco importante da normação da União Europeia foi a Directiva (EU) 2016/1148 do Parlamento e do Conselho, de 6 de Julho. Este diploma previa medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Entre essas medidas, sem pretensões exaustividade, encontramos: a identificação dos operadores de serviços essenciais (art. 5º); o dever de adopção, por parte dos Estados-Membros, de estratégias nacionais de segurança das redes e dos sistemas de informação (art. 7º); o dever de os Estados-Membros designarem autoridades nacionais competentes no que respeita à segurança das redes e dos sistemas de informação (art. 8º); a criação, por parte dos Estados-Membros de equipas de resposta a incidentes de segurança interna (art. 9º); regras relativas a requisitos de segurança das redes e dos sistemas de informação, bem como regras relativas à notificação de incidentes (art. 14º); o incentivo da normalização dos procedimentos dos Estados-Membros (art. 19º); a previsão de normas sancionatórias (art. 21º).

A Directiva em análise revela particular preocupação com a economia da União, com a estabilidade do Mercado Interno, encontrando-se voltada essencialmente para entidades privadas, nomeadamente os bancos e as infra-estruturas financeiras. Nesta óptica de equilíbrio – nem sempre conseguido[29] – entre os actores públicos e privados da cibersegurança, o diploma em estudo sublinha a necessidade de uma boa gestão das cibercrises. Uma gestão que passa pela partilha de informações entre agentes públicos e privados a propósito de incidentes de cibersegurança, de exercícios que simulam cenários de crise – como o "Cyber Europe" promovido pela ENISA –, e pelo reforço da segurança do "hardware" e do "software" dos operadores em questão. Tal como havíamos visto na Convenção de Budapeste, a Directiva 2016/1148 reforça a necessidade do estreitamento da cooperação internacional em matéria de cibersegurança.

[29] Refira-se que a Directiva parece demonstrar maior preocupação com o Mercado Interno do que com a Defesa e a Segurança propriamente ditas, promovendo talvez um maior enfoque na política geral do que na política criminal.

## 5. A cibersegurança no contexto português

Em 2018, a Directiva 2016/1148 foi transposta para o ordenamento jurídico português através da Lei nº 46/2018, de 13 de Agosto (Regime Jurídico da Segurança do Ciberespaço). Porém, andes de nos adentrarmos na Lei nº 46/2018, façamos algumas considerações em torno da adequação contemporânea do binómio segurança-liberdade. Muito antes da transposição da Directiva que nos ocupa, o legislador vinha a reflectir sobre as implicações das ameaças cibernéticas no binómio segurança-defesa. Assim, através do Conceito Estratégico de Defesa Nacional – conjunto de orientações referentes à política de defesa nacional –, começou a compreender que as diversas ameaças informáticas não constituem apenas um problema de segurança, mas igualmente uma questão de defesa.

Semelhante percepção teve origem nas ameaças cibernéticas dirigidas às infraestruturas críticas do Estado. Como referimos anteriormente, a cibercriminalidade poderá lesar ou colocar em perigo a segurança de diversos sistemas essenciais à manutenção do Estado (justiça, saúde, educação, segurança social, etc.). Nesta óptica, as ameaças cibernéticas dirigidas às estruturas essenciais do Estado, mais do que inquinar a paz jurídica, ou seja, mais do que desestabilizar as expectativas comunitárias na vigência da norma violada, colocam em causa o próprio *status quo* estatal. Não queremos com isto significar que que as ciber-ameaças se apartaram do âmbito jurídico-penal a favor do direito dos conflitos armados. Queremos significar, ao invés, que a política criminal hodierna deve preferir uma abordagem interdisciplinar do fenómeno criminal, uma abordagem que não se reduza aos estreitos limites do direito penal, mas que aceite o contributo de outras áreas do saber jurídico como será o caso do direito da defesa nacional[30]. Pelo exposto, a cibersegurança convoca preocupações comuns aos cultores das ciências criminais e da defesa nacional, pelo que talvez seja de ponderar a substituição do consabido binómio segurança-liberdade pelo trinómio segurança-liberdade-defesa. Não tanto, diga-se, como se a liberdade

[30] Numa aproximação ao direito da defesa nacional, ver GOUVEIA, Jorge Bacelar – *Defesa Nacional e Forças Armadas: Uma perspetiva do Direito Militar da Segurança em Estado Constitucional Democrático.* Coimbra: Almedina, 2022, pp. 135 e ss.

passasse a obedecer a dois *dominus*, mas na perspectiva da construção de um verdadeiro sistema global de justiça penal, um sistema de justiça que não afaste o contributo de nenhuma área do saber jurídico e do pensamento político-criminal em sentido amplo.

Voltemos a 2018 e ao Regime Jurídico da Segurança do Ciberespaço que transpôs a Directiva 2016/1148 para o ordenamento jurídico português. De acordo com o seu art. 2º, nº 1, o Regime aplica-se à administração pública, aos operadores de infraestruturas críticas e de serviços essenciais, aos prestadores de serviços digitais e a quaisquer outras entidades que utilizem redes e sistemas de informação. Em suma, aplica-se tanto a entidades públicas como privadas. Diga-se igualmente que o Regime previu o Conselho Superior de Segurança do Ciberespaço (art. 5º), órgão consultivo do Primeiro Ministro, bem como o Centro Nacional de Cibersegurança (art. 7º), que exerce funções de regulação, regulamentação, supervisão, fiscalização e que possui igualmente competências sancionatórias em relação às redes e aos sistemas de informação. Mais criou uma equipa de resposta rápida a incidentes de segurança informática nacional, a CERT.PT (art. 8º), tal como mecanismos de reporte obrigatório de incidentes de cibersegurança para entidades públicas e privadas (art. 12º e ss).

Note-se que a lei portuguesa parece ter ido além da Directiva e reconheceu a importância da ciber-espionagem, da ciberdefesa, do ciber-crime e do ciberterrorismo. Encontra-se, portanto, em linha com as preocupações mais recentes em termos de cibersegurança e, uma vez mais, voltamos a deparar-nos com a íntima conexão entre a segurança e a defesa ou, para sermos mais precisos, com o trinómio segurança-liberdade-defesa.

## 6. A Estratégia Nacional de Segurança do Ciberespaço

De acordo com o art. 4º, nº 1 do Regime Jurídico da Segurança do Ciberespaço, "[a] Estratégia Nacional de Segurança do Ciberespaço define o enquadramento, os objectivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional". Trata-se de um documento plurianual que contém um conjunto alargado de orientações de política geral e de política criminal. Ademais, como parece resultar da norma citada e adiante veremos

com maior propriedade, a Estratégia centra-se, não apenas na segurança, mas igualmente na defesa.

A Estratégia Nacional de Segurança do Ciberespaço (2019-2023), adoptada pela Resolução do Conselho de Ministros nº 92/2019, de 23 de Maio, reconhecendo a desactualização da Estratégia anterior (2015), demonstrou preocupação com o rápido desenvolvimento do ciberespaço e com a progressão das respectivas ameaças. Como indicámos anteriormente, a Estratégia vai além da política criminal, referindo a relevância da consecução da prosperidade social. De facto, o documento identifica o ciberespaço "como domínio de desenvolvimento económico, social, cultural e de prosperidade". Talvez pudéssemos ir mais longe e aprofundar o elo que parece existir entre a prosperidade e a maior ou menor incidência das ciber-ameaças, mas semelhante desiderato ultrapassa os limites do nosso objecto de estudo.

Ainda na óptica da segurança, a Estratégia alerta para a relevância do reforço do Estado de direito democrático e do regular funcionamento das instituições. Como vimos anteriormente, trata-se de um receio fundado na potencialidade normativamente erosiva das ameaças e do perigo das respostas neopunitivas ou hipercriminalizantes. No âmbito da defesa, não devemos ignorar que a Estratégia se debruça sobre os riscos geopolíticos, os conflitos armados e o terrorismo. Trata-se de uma visão de largo espectro que não deixa de fora novas abordagens como a ciberdiplomacia, como adiante veremos.

Voltando ao âmbito da segurança, o instrumento em crise sublinha a proliferação do "malware", do "ransomware" e o crescimento da "internet das coisas", desafios novos que, como referimos anteriormente, a pós-modernidade não cessa de colocar aos operadores jurídicos. Diga-se, por fim, que a estratégia frisa também a fraca cultura de cibersegurança e de responsabilidação individual da sociedade portuguesa.

Encontrando-se ancorada nos princípios da subsidiariedade, da complementaridade e da proporcionalidade – no seu tríplice entendimento de necessidade, adequação e proporcionalidade em sentido estrito –, a estratégia desenvolve-se através de 6 Eixos de actuação, a saber:

a) O **Eixo 1** contende com a estrutura de segurança do ciberespaço que se encontra prevista no art. 5º e ss. do Regime Jurídico da Segurança do Ciberespaço. Neste sentido o Eixo

1 prima pelo reforço do Conselho Superior de Segurança do Ciberespaço e do Centro Nacional de Cibersegurança "como ponto de contacto único nacional para efeitos de cooperação internacional em matéria de cibersegurança". Refira-se ainda que o presente âmbito pugna pelo reforço das estruturas e capacidade de actuação do Ministério Público, da Polícia Judiciária, das Forças Armadas e dos Serviços de Informações. Notemos a diversidade de actores a marcar a Estrutura de Segurança e a denotar a complexidade da tarefa em causa. Uma vez mais, encontramos a segurança e a defesa num claro plano de proximidade.

b) O **Eixo 2** centra-se na prevenção, educação e sensibilização. Trata-se de um Eixo de suma importância por recentrar a prevenção num estádio pré-delitivo e não exclusivamente criminal. Ao colocar o enfoque nos diversos níveis de ensino, a Estratégia reconhece as virtualidades preventivas da educação ou, dito de outro modo, reconhece que a prevenção criminal deve ter início muito antes da comissão do facto, constituindo uma tarefa que deve convocar e ocupar toda a sociedade. Trata-se de uma concepção ampla da política-criminal, uma concepção que não olvida a dimensão social da cultura ou da aculturação como elemento essencial de uma cidadania verdadeiramente inclusiva. A relevância que outrora se atribuiu às campanhas de alfabetização deve ser hoje dispensada para outros analfabetismos funcionais ou iliteracias. Neste sentido, a educação apresenta-se como um instrumento essencial para garantir a literacia digital[31], num duplo sentido. Por um lado, ao alertar os cidadãos para as ameaças cibernéticas, ensinando boas práticas que devem ser adoptadas no contacto com a tecnologia. Por outro lado, ao alertar as comunidades-alvo para os efeitos profundamente

[31] Para uma explicitação sumária da origem da expressão "literacia digital", cfr. SECKER, Jane – *The trouble with terminology: rehabilitatinh and rethinking 'digital literacy'*. In Reedy, Katharine;Parker, Jo – Digital Literacy Unpacked. London: Facet Publishing, 2018.

desestabilizadores das ameaças cibernéticas, explicando o seu real impacto em termos de lesão ou de colocação em perigo de bens jurídicos. Notemos, no entanto, que o presente Eixo não incide apenas sobre os diversos níveis de ensino. Ao invés, contém um escopo mais amplo, na medida em que não ignora as necessidades formativas profissionais no âmbito da cibersegurança, bem como a capacidade de rendimento de "programas de sensibilização específicos junto das instituições públicas e privadas". Não pecaremos por excesso ao afirmar que a prevenção pré-delitiva, mais especificamente as medidas que incidam na formação e sensibilização da sociedade e das comunidades que a constituem, deve constituir a grande aposta político-criminal do futuro, no exacto sentido do afastamento de abordagens meramente reactivas ou vincadas por linguagem belicosa (combate, repressão, controlo, etc.).

c) O **Eixo 3**, referente à protecção do ciberespaço, incide igualmente sobre a prevenção, bem como sobre a detecção, resposta e recuperação da ameaça. Mais reforça a necessidade da promoção de "estruturas de cooperação nacional e sectorial de proteção do ciberespaço", tanto do sector público como do privado. O presente Eixo atesta a relação de identidade entre a segurança do ciberespaço, a segurança nacional e o regular funcionamento do Estado.
d) O **Eixo 4** contende com a resposta às ameaças e o combate ao cibercrime, incidindo particularmente, e uma vez mais, na prevenção e na dissuasão, ou seja, da dimensão pré e pós-delitiva da cibersegurança. A Estratégia insiste no reforço e actualização legislativa, tendo em conta o surgimento de novas tipologias de crime e também de "crime antigos com novos métodos e acções ofensivas de grande envergadura lesivas do interesse nacional".
e) O **Eixo 5**, que contempla a investigação, desenvolvimento e inovação, merece especial menção por visar promover a união de esforços entre a academia, entidades do sector público e privado e do tecido empresarial. Pese a referência

algo redundante ao "tecido empresarial", que se integra naturalmente nas entidades do sector público ou privado, não podemos deixar de reputar como muito importante a inclusão do conhecimento teorético-prático no âmbito da prevenção do cibercrime. De facto, a produção de conhecimento releva-se essencial para a adequada delimitação de instrumentos político-criminais preventivos, principalmente em áreas emergentes e de rápida expansão como a cibersegurança. Acresce que, no que respeita à academia, constitui uma relevante oportunidade para promover a transição do "direito nos livros" para o "direito em acção". A Estratégia clarifica ainda que a produção científica pode ser um dos instrumentos para a promoção da independência nacional em matéria de cibersegurança. E, uma vez mais na óptica da cooperação, reforça a necessidade da criação de "sinergias" com a União Europeia e a Organização do Tratado Atlântico Norte o que, como vimos incansavelmente a reiterar, significa pensar o problema das ciber-ameaças não apenas na óptica da segurança, mas também da defesa.

f) Finalmente, reforçando o signo da cooperação nacional e internacional, o **Eixo 6** incide sobre um "mundo altamente ligado e interdependente" e apresenta como actores privilegiados da cooperação europeia e internacional a União Europeia, a Organização da Nações Unidas e a Organização do Tratado Atlântico Norte. Neste âmbito extraterritorial, reforça a importância da ciberdiplomacia e das parcerias estratégicas no espaço lusófono.

De modo a encerrarmos o presente excurso, refira-se ainda que a Estratégia é implementada por via de um Plano de Acção que possibilita o acompanhamento individualmente das medidas a implementar e garante uma visão de conjunto das mesmas. O Plano permite igualmente analisar a progressão anual das medidas em curso, compreendendo em que fase do período de execução se encontram. Por fim, possibilita a compreensão e a ponderação dos resultados atingidos, dos objectivos não cumpridos e dos

desvios verificados. Como é bom de ver, a relação biunívoca que se estabelece entre a Estratégia e o Plano permite que aquela não se revele um instrumento meramente semântico mas que possa ser aplicada na prática, que se possa realizar quotidianamente no desafio e na exigência das ameaças concretas. O acompanhamento e avaliação das medidas previstas na Estratégia permite radiografar a adequação do exercício e trilhar um caminho que se manifeste na optimização do instrumento que lhe suceda e que, no presente momento, se encontra em preparação.

## 7. Concluindo

Ao longo das últimas décadas as percepções axiológicas da comunidade e o próprio tratamento jurídico das questões relacionadas com a cibersegurança têm sofrido alterações de monta. Longe vão os tempos em que o mundo digital surgia próximo de um cenário de ficção científica, firmado num exotismo que o afastava definitiva e terminantemente do mundo dito real. Hoje é possível afirmar que o exotismo do estranhamento que acompanha sempre as novidades deu lugar à convivência. Uma convivência quotidiana com a tecnologia que afasta as visões mediadas ou meramente aproximativas fundadas em preconceitos sobre o mundo digital, fundeadas em percepções de insegurança mais do que na verdadeira insegurança[32].

Hoje a incerteza do futuro tecnológico num mundo globalizado deu lugar à certeza da digitalização do tráfego social, à certeza de que o mundo digital e o mundo físico não devem ser perspectivados como duas realidades refractárias. Aliás, começa a surgir a suspeita de que a dualidade de mundos deu lugar a uma mundividência una ou unificada, uma mundividência que não distingue entre mundo físico e mundo digital. Neste sentido, os sistemas de justiça não devem permanecer alheios aos problemas de segurança que surgem e se desenvolvem no mundo dito digital, na medida em que estes desafios não se encontram encerrados numa rede computacional sem contacto

[32] Numa análise recente das percepções públicas sobre o cibercrime, cfr. GUEDES, Inês Sousa; MOREIRA, Samuel; CARDOSO, Carla – *Cibercrime: Conceptualização, desafios e percepções públicas*. In Guedes, Inês Sousa;Gomes, Marcus Alan de Melo – Cibercriminalidade: Novos Desafios, Ofensas e Soluções. Lisboa: Pactor, 2021, pp. 11 e ss.

com a realidade (autopoiética e auto-referente). Pelo contrário, as ameaças cibernéticas contendem directamente com a estabilidade estatal, colocando em risco os seus diversos sub-sistemas ou infra-estruturas essenciais e, como corolário necessário, ameaçando a conceção do Estado de direito em sentido material que tem enformado a *forma mentis* jurídica ocidental. Uma *forma mentis* que não abdica nem deve abdicar da configuração aberta e pluralista dos Estados, configuração esta que tem vindo a ser colocada em causa pela proliferação das ciber-ameaças ou, dito de outro modo, pela exponenciação das zonas fronteiriças globais, para regressarmos à lição de Bauman.

As zonas fronteiriças globais ou, se preferirmos, as dimensões do mundo digital avessas à normação estatal (não-Estado ou contra-Estado) colocam em evidência que não existe um Rubicão a separar o cibermundo do mundo físico, a cibersegurança da segurança, nem existe tampouco uma resposta normativa unidimensionalmente eficaz. Ademais, como foi nosso desiderato aclarar ao longo deste breve excurso, as ameaçar cibernéticas não se perfilam apenas como um problema de segurança, mas invocam igualmente a questão da defesa. Neste sentido, o binómio segurança-liberdade vê-se substituído pelo trinómio segurança-liberdade-defesa que aumenta não apenas a complexidade problemática mas também o risco de contaminação da liberdade. Dito de modo claro, para além do risco de colonização do tecido social – do mundo da vida – pelas ameaças cibernéticas, não devemos descartar o risco de degradação das esferas de liberdade dos cidadãos por via da hipertrofia normativa.

A preocupação em torno dos avanços tecnológicos tem levado os legisladores europeu e nacional a abordar a questão da cibersegurança de modo complexivo. Destarte, a cibersegurança tem vindo a ser pensada como um problema de justiça a convocar diversas áreas do labor normativo, bem como dimensões do saber não jurídico. Sob semelhante prisma, a política criminal emerge como um dos instrumentos privilegiados na redução problemática das ciber-ameaças. Uma política criminal que, por um lado, não ignora ou afasta os contributos do direito penal (substantivo e adjectivo) nem da criminologia e que, por outro lado, não contende apenas com a prevenção criminal pós-delitiva, também designada (questionavelmente) como reacção ou repressão criminal. Ao invés, referimo-nos a uma política criminal que pensa as ciber-ameaças no seu contexto espácio-temporal, uma política criminal que incide principalmente sobre o estado prévio à comissão do crime, não com o fito de

erguer um direito penal de guarda avançada, mas através da delimitação de instrumentos e estratégias verdadeiramente preventivos, capazes de actuar num estádio pré-delitivo, incidindo sobre potenciais agentes e vítimas.

Na óptica do desenvolvimento de uma política criminal sustentada e comprometida com as diversas comunidades que compõem a sociedade, reputamos importante o labor normativo do legislador da União Europeia e do legislador nacional em torno da cibersegurança, principalmente no que respeita ao Regime Jurídico da Segurança do Ciberespaço e da Estratégia Nacional de Segurança do Ciberespaço. Reputamos importante, na medida em que os instrumentos em causa apostaram na mencionada abordagem político-criminal abrangente e que privilegia a prevenção sobre o "combate".

Numa altura em que a actual Estratégia Nacional de Segurança do Ciberespaço se aproxima do término, seria importante encetar algumas reflexões retrospectivas e prospectivas. Em primeiro lugar, urge reconhecer a imbricação entre a segurança e a cibersegurança, entre a segurança e a defesa, e entre o mundo digital e o mundo físico. Cabe igualmente reconhecer que as respostas normativas devem evitar a dispersão e que o legislador deve continuar a investir na senda da prevenção ao invés da mera repressão, tão cara a programas de política geral neopunitivos e populistas pouco preocupados com aquele que deve ser o escopo político-criminal de um Estado de direito em sentido material, a saber, a prevenção geral positiva e a prevenção especial positiva. Pelo exposto, cabe revelar preocupação, não apenas com a colonização anómica do ordenamento jurídico pelas ameaças cibernéticas, mas também com a colonização ou, dito com maior clareza, com a contaminação da política criminal pela política geral. Em suma, a cibersegurança deve ser pensada e abordada, não com o estranhamento de antanho, mas com a desenvoltura do pensamento sistémico, com o olhar desimpedido da busca por um verdadeiro sistema de justiça penal. De volta "Mundo no Arame" ou ao "Matrix", tememos que a sua lição esteja ultrapassada. Hoje a personagem principal destes filmes não despertaria na consciência de que viveu um simulacro de mundo, uma experiência de demiurgo, uma contrafacção da realidade. Hoje a personagem principal despertaria consciente de que não existe diferença entre o sonho e vigília, o mundo digital e o mundo real. Despertaria com a certeza de que o mundo digital e o mundo real mais não são do que duas facetas da mesma realidade, carecidas de tratamento sistémico e sistemático.