REGULAMENTAÇÃO SUPRANACIONAL SOBRE CRIMINALIDADE INFORMÁTICA E TÉCNICAS DE TRANSPOSIÇÃO. O DIREITO PENAL PORTUGUÊS E ESPANHOL COMO PARADIGMAS

Francisco Proença de Carvalho, Oscar Morales García e Manuel Álvarez Feijoo
*Abogados**

Regulamentação supranacional sobre Criminalidade Informática e Técnicas De Transposição. O Direito Penal Português e Espanhol como Paradigmas

A expansão das tecnologias da informação, e em particular da Internet, favoreceu o processo de globalização económica e cultural e, consequentemente, o progresso. Ao mesmo tempo, novas formas de violação de bens jurídicos, clássicos e emergentes, desencadeiam desafios de difícil resposta dado o carácter transfronteiriço do fenómeno. No âmbito supranacional, foram duas as instituições que apresentaram um inequívoco espírito de construção legislativa tendente à harmonização: O Conselho da Europa e a União Europeia. O presente trabalho analisa as propostas legislativas de ambas as instituições, assim como o modelo de transposição seguido por Espanha e Portugal.

International models for the transposition of supranational cybercrime rules. Spain and Portugal as a paradigma

The expansion of information technologies, particularly of the Internet, has stimulated the cultural and economic globalization process and the subsequent social development. At the same time, both classical and emergent legal interests are under new forms of attack (or cyberattack) which trigger harsh challenges in the context of a cross-border phenomenon. Two supranational institutions have shown an unambiguous willingness to build a harmonized legislation in the field of cybercrime: the Council of Europe and the European Union. This paper deals with the legislative proposals of both institutions and analyses the national transposition models applied by Spain and Portugal.

Palavras chave
Cibercrime, Informática, Transposição, Cooperação internacional, Convenção de Budapeste.

Key words
Cybercrime Computer crime, Convention of Budapest, Information, technologies, Hacking.

Fecha de recepción: 15-1-2018 *Fecha de aceptación: 15-5-2018*

1 · O CONSELHO DA EUROPA E A UNIÃO EUROPEIA: A CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME E AS DIRETIVAS EUROPEIAS SOBRE SEGURANÇA INFORMÁTICA

A emergência do fenómeno tecnológico, a sua generalização e democratização, oscilou entre a liberdade enquanto máxima nos momentos iniciais e o intervencionismo atual, quando a técnica revelou possibilidades de controlo institucional mais do que sugestões[1]. Sem dúvida, a denominada *Sociedade de Informação* que nasce ao abrigo das tecnologias - não apenas as de caráter telemático, como também de outro tipo, como o cabo ou a televisão digital - veio transformar as relações sociais e jurídicas de um modo incontestável e impressionante[2]. A evolução tecnológica permite um incremento da qualidade de vida; mas, do mesmo modo que se constatam alterações na estrutura e desenvolvimento social e económico, ao mesmo tempo abre-se a porta a novas formas de prejudicar os legítimos interesses alheios, quer sejam individuais ou coletivos[3].

O caráter transfronteiriço das tecnologias da comunicação deu origem a uma necessidade precoce da criação de normas internacionais de harmonização do fenómeno. Dentro desta lógica, nasceu o projeto legislativo mais ambicioso sobre a matéria, a Convenção do Conselho da Europa sobre o Cibercrime que, por sua vez, serviu para a União Europeia iniciar, ainda que mais lentamente, o seu dispositivo regulamentar.

* Del Área de Derecho Público, Procesal y Arbitraje (Barcelona y Lisboa)

1 *Vid.* uma análise da evolução institucional relativamente à expansão tecnológica em MORALES GARCÍA, O., "Criterios de atribución de responsabilidad penal a los prestadores de servicios de la sociedad de la información", em *Revista de Derecho y Proceso Penal*, n.º 5, 2001, pp. 140 e ss., e bibliografia aí citada.

2 A ideia em geral é amplamente desenvolvida em CASTELLS, M., *La era de la información. Economía, sociedad y cultura. Vol. I La sociedad red*, Tradução de Carmen Martínez Gimeno, 1997, *passim*. *Vid.*, entre outros, FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías, Internet y Derechos Fundamentales*, 1998, p. 23; CAPELLER, W., *Not such a Neat Net. Some comments on virtual criminality*, 2000, p. 3

3 Reflexão genérica que, em relação à denominada *sociedade de riscos* ou *sociedade pós-industrial,* pode ver-se em SILVA SÁNCHEZ, *La expansión del Derecho Penal. Aspecto de la política criminal en las sociedades postindustriales*, 1999, p. 22.

Com caráter prévio à aprovação da Convenção de Budapeste, a passagem para a sociedade de informação também não havia passado despercebida ao Conselho, de onde tinham sido emanados textos com eficácia normativa limitada, mas de indubitável peso político, como as Recomendações (87) 15 sobre a utilização de dados pessoais ou a (95) 4 relativa à tutela dos dados pessoais no âmbito das Telecomunicações. Alinhado com esta trajetória, em novembro de 1996, "o Comité Europeu para os problemas criminais", isto é, o órgão do Conselho da Europa encarregado de elaborar a política criminal da Instituição, alertado para a vertiginosa evolução tecnológica e novas ameaças à segurança e consequentes novos riscos para bens jurídicos de primeira ordem, como a privacidade ou o património, adotou a decisão de criar um comité de especialistas para trabalhar sobre o fenómeno da delinquência associada à tecnologia, e isso sob uma máxima, sem dúvida presente nas primeiras versões da Convenção: a dependência social, económica e cultural da informação constante das redes de comunicação, particularmente na Internet, obriga à tutela dos bens jurídicos fundamentais que se encontram em jogo; por fim, de acordo com a filosofia segundo a qual a sucessão história do modelo de sociedade, na qual agora todos podemos ser sujeitos ativos e passivos da informação, reclama uma regulamentação (também) penal harmonizada e global, assim como global é a sociedade de informação.

Em 1997, o Comité de Ministros nomeou um Comité de Especialistas em criminalidade informática no ciberespaço, no qual se estabeleceu como data limite para a finalização dos seus trabalhos e entrega de uma proposta ao Comité o dia 31 de dezembro de 1999, prazo que foi prorrogado por um ano. A 27 de abril de 2000, os trabalhos preparatórios foram desclassificados, tornando pública e aberta a discussão a versão n.º 19, amplamente modificada até à redação da última e definitiva versão 25.2, aprovada em junho de 2001 pelo Plenário do Comité de Ministros do Conselho da Europa, e aberta para assinatura a 23 de novembro de 2001, na reunião do Conselho da Europa em Budapeste.

A estrutura, conteúdo e alcance da Convenção naquele momento pode ser explicada cabalmente pela falta de iniciativas internacionais ou supranacionais nesta matéria, o que na altura propiciou a tomada de decisões de especial importância sobre a Convenção:

a) Em primeiro lugar, a decisão de trabalhar sobre uma Convenção e não tanto sobre uma Recomendação, dada a necessidade de harmonizar a legislação dos diversos países pertencentes ao Conselho da Europa, não apenas em matéria penal substantiva, como também no âmbito processual e de colaboração administrativa internacional, isto é, coordenação da ação policial, recolha de dados da investigação criminal, etc.[4]

b) Em segundo lugar, a decisão de alargar a assinatura da proposta a países não pertencentes ao Conselho da Europa, e cuja participação ativa condicionou, sem dúvida, parte da estrutura e conteúdo do articulado[5]. Na realidade, a minuta da Proposta do Conselho da Europa de 27 de abril de 2000, assumiu, em cada um dos âmbitos de afetação, políticas de limites máximos nas quais a cessão de garantias sobre os poderes públicos foi destacada em inúmeras instituições[6]. Facto esse que veio gerar consideráveis tensões com a União Europeia que, na altura, era menos proclive em matéria de delinquência informática. Estas tensões acabariam, paradoxalmente, com o Conselho a renunciar as suas pretensões mais agressivas que, no entanto, mais tarde, seriam igualmente absorvidas, pela UE.

Devido à sua própria estrutura de funcionamento, a União Europeia não aparece como uma organização capaz de criar um texto global que harmonize as diversas legislações dos Estados-Membros no que se refere à criminalidade informática. Assim, perante a Convenção do Conselho da Europa, a União foi criando um conjunto inicial de Pareceres, Decisões-Quadro e Diretivas sectoriais que já pouco diferem do Texto aprovado no seio do Conselho da Europa. A todos faremos referência em seguida, a propósito da estrutura da Convenção.

---

4 Na base desta decisão, tal como se reconhece na Exposição de Motivos da Convenção, está o estudo do professor Kasperson intitulado *"Implementation of Recomendation Nº R (89)9 on computer-related crimes"*, realizado a pedido do próprio Comité de especialistas. A exposição de motivos pode ser consultada online em http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

5 Nomeadamente, participaram ativamente na redação das diversas minutas e no texto definitivo, os Estados Unidos, o Canadá, a Austrália e o Japão, entre outros.

6 *Vid*., em http://www.gilc.org/privacy/coe-letter-1000-es.html a declaração emitida a 13 de outubro de 2000 pela *Global Internet Liberty Campaign*, integrada por um conjunto de grupos de caráter civil com peso específico nos processos de tomada de decisões, como a *American Civil Liberties Union*, ou o *Electronic Privacy Information Center (EPIC)*, entre outros.

1.1 · Harmonização da cooperação internacional policial e processual

Duas foram as questões de maior interesse relativamente às quais, por sua vez, a União Europeia foi capaz de legislar em maior ou menor medida.

1.- Cessão às autoridades administrativas de parcelas de autogestão no uso das tecnologias, como o acesso não autorizado a máquinas, para efeitos exclusivos de investigação criminal, sem concessões aos aspetos essenciais de preservação da informação. A União Europeia, através do Parecer 4/2001, sintetizou a sua preocupação sobre a participação na Convenção de países não pertencentes ao Conselho da Europa e, portanto, à sua tradição jurídica. Desta forma, enquanto os países pertencentes à União Europeia transpuseram para o seu Direito interno as diversas diretivas emanadas do Parlamento sobre a tutela de dados pessoais, e inclusive os países pertencentes à órbita do Conselho da Europa assumiram a política inerente às Recomendações sobre a mesma matéria, os Estados não pertencentes à UE ou ao Conselho da Europa não se encontravam vinculados à referida regulamentação. Daí que, além da evidente divergência filosófica na tutela dos dados pessoais existentes entre a Europa e os Estados Unidos, a cessão implicasse a possibilidade de que cada Estado facultasse a outro os dados pessoais obtidos num país da União ou do Conselho, no decurso de uma investigação criminal, mesmo no caso em que o cessionário oferecesse uma tutela jurídica muito inferior à exigida nesses territórios, quebrando-se, desta forma, a pretensão harmonizadora e deixando para a legislação interna a salvaguarda efetiva dos direitos fundamentais. As amplíssimas concessões em matéria de dados de caráter pessoal estendiam-se, não apenas aos obtidos no decurso de uma investigação policial, como também à cessão de dados necessária para a investigação em países fora do território do Conselho, obrigatória a partir do momento em que fossem solicitadas por um Estado parte da Convenção e cuja evasão seria exequível unicamente por reserva prévia e expressa da eficácia do preceito, assente em motivos de ordem pública ou relativos à segurança e defesa nacionais. Além disso, a União Europeia destacou no citado parecer como através do artigo 15 da Minuta, na sua redação de 27 de abril de 2000, que "poderia gerar-se a impressão de que a tutela dos Direitos Fundamentais seria apenas observada quando fosse devida e em qualquer caso de forma apenas 'adequada'". Ademais, considerações sobre a proporcionalidade dos poderes ou procedimentos de acordo com a natureza e circunstâncias da conduta investigada não são contempladas como princípio geral de atuação, refere-se apenas que devem ser unicamente observadas no caso de serem aplicáveis em geral. Interpretados como uma limitação das garantias e procedimentos, os direitos fundamentais eram entendidos como infralegalmente protegidos, se não mesmo como absolutamente desprotegidos. A evolução do texto até uma versão definitiva, porém, ultrapassou esta preocupação.

2.- Obrigação dos prestadores de serviços da Sociedade de Informação de registar a atividade dos utilizadores e armazenar os dados resultantes, com o consequente risco para a privacidade e para os dados pessoais dos utilizadores e o normal funcionamento das redes telemáticas, obrigação esta, não obstante, finalmente excluída do texto definitivo do Tratado, principalmente por falta de acordo entre a União Europeia e o Conselho da Europa[7]. É precisamente neste ponto que a UE atravessa um dos seus episódios de política criminal de maior oscilação. A primeira abordagem da União a este fenómeno ocorreu com a Recomendação 3/1999 sobre a conservação dos dados de tráfego pelos Fornecedores de Serviços de Internet, por meio da qual a UE, ainda antes da primeira versão da Convenção tornada pública pelo Conselho da Europa, manifestava a sua oposição a medidas de intervenção sobre o tráfego de dados. A Recomendação, elaborada pelo então denominado "Grupo do artigo 29[8]", expressou a sua preocupação em relação ao armazenamento de dados nos diversos países membros da UE. Consciente da necessidade de controlar os dados que circulam através de um servidor para poder efetuar os trabalhos oportunos de registo de

7 Como assinalou LEZERTÚA, M., "El Proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", em LÓPEZ ORTEGA (Director), *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, 2001, pp. 34 e ss., existe uma evidente distância entre os primeiros projetos da Convenção e a versão definitiva; diferenças que, no que respeita às medidas de atuação processual contra a delinquência informática e, em particular, ao armazenamento de dados, o seu arquivo, exibição, entrada e registo ou a interceção em tempo real de dados de tráfego ou conteúdo (arts. 15 a 19), permitem uma avaliação positiva, dado que definitivamente tais medidas se coadunam com o princípio de proporcionalidade como eixo cartesiano, assim como com o nível de garantias do direito interno.

8 Denominou-se assim o Grupo de especialistas para a tutela das pessoas relativamente ao tratamento de dados de caráter pessoal, criado em virtude do disposto no artigo 29 da revogada **Diretiva 95/46/CE**, do Parlamento, sobre a tutela das pessoas singulares em relação ao tratamento dos dados pessoais e a livre circulação dos dados.

acordo com os dados reunidos, o Grupo conciliou, além disso, as necessidades de investigação criminal em tempo real, com indemnidade dos bens jurídicos subjacentes. Na verdade, o Grupo considerou na Recomendação que o facto de que um terceiro possa vir a estar na posse de informação decorrente do tráfego de dados através de um servidor implicaria uma violação de um direito fundamental, o que, em geral, constituiria crime, salvo se a medida de interceção da comunicação ou do seu conteúdo cumprisse as exigências jurídicas típicas da afetação de Direitos Fundamentais reunidas nas diversas Convenções sobre os Direitos do Homem, isto é, proporcionalidade da medida, apenas adotável onde não existam outros mecanismos alternativos para o desenvolvimento da investigação, assim como um fundamento claro para a sua adoção, no qual se deveriam refletir tanto a duração, finalidade, meios técnicos e limites da interceção a aplicar. A conclusão idêntica se chega sobre a política (criminal) em matéria do tráfego de dados pelos fornecedores de serviços a partir da leitura da Diretiva 2000/31/CE, de 8 de junho, do Comércio eletrónico, que, de forma alguma, impôs tal obrigação aos fornecedores de serviços. A União Europeia seguiu esta lógica também na Diretiva 2002/58/CE, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, cujos artigos 5, 6 e 9 proibiam a retenção de dados de tráfego para além das necessidades de faturação entre empresas. Seria a Diretiva 2006/24/CE, de 15 de março, sobre a conservação de dados gerados ou tratados relativamente à prestação de serviços de comunicações que, no quadro do Primeiro Pilar (comércio), ordenaria aos Estados-Membros a retenção indiscriminada de dados das comunicações para efeitos de combate ao terrorismo e à criminalidade organizada. Na sua sentença de 8 de abril de 2014 (*Digital Rights Ireland e Stelinger*) o TJUE declararia a nulidade da citada Diretiva, por exceder o princípio de proporcionalidade em relação à afetação do direito à privacidade dos cidadãos da União. Mais adiante, inclusivamente, o TJUE proferiu sentença a 21 de dezembro de 2016 declarando nulas as normas nacionais de transposição da diretiva que foram o reflexo fiel do seu conteúdo.

1.2 · Harmonização de direito substantivo

1.- Crimes contra a integridade dos sistemas. Nesta categoria são incluídos tanto crimes de acesso ilegal a sistemas, como os de danos informáticos e interrupção do funcionamento dos sistemas. O Conselho da Europa parte da necessidade de tipificar o acesso ilegal a sistemas e a interceção de comunicações, optando, preferencialmente, em relação à primeira modalidade, por uma descrição o mais objetiva possível no que concerne a conduta, ou seja, despida de ingredientes acrescentados ao próprio acesso, de caráter objetivo (com violação de medidas de segurança), assim como de caráter totalmente subjetivo (finalidade conhecer a privacidade, etc.). Trata-se de proporcionar uma declarada tutela não tanto à privacidade dos cidadãos, mas principalmente à integridade dos sistemas. Do mesmo modo, a Decisão-Quadro de 19 de abril de 2002, sobre os ataques de que podem ser objeto os sistemas de informação, recomendava aos Estados-Membros da UE a harmonização da legislação penal nesta matéria, tipificando, em matéria de acesso abusivo, as condutas consistentes em aceder a um sistema apenas quando as medidas de segurança tivessem sido violadas; e, no caso de estas não existirem, caso o acesso tivesse sido realizado com a finalidade de causar *danos às pessoas singulares ou jurídicas.* Mais tarde, a Diretiva 2013/40/UE, de 12 de agosto viria a substituir a anterior Decisão-Quadro, integrando um sistema de tutela idêntico ao da Convenção, inclusive em matéria de interceção de emissões eletromagnéticas, omitida na primeira, com uma redação aperfeiçoada de alguns tipos, produto, sem dúvida, da evolução do comportamento dos cidadãos nos últimos e intensos (tecnologicamente) doze anos que decorreram desde a aprovação da Convenção.

No mesmo sentido, tanto a Convenção como a Diretiva de 2013, reclamam uma ampla proteção da causalidade de resultados danosos, com antecipação de tutela incluída. Reclama-se a criação de tipos de infrações penais em cascata, nos quais se tutele (i) a integridade da informação (apagamento); (ii) a interrupção do funcionamento dos sistemas que não deteriora definitivamente, mas apenas temporariamente os sistemas; (iii) e o fabrico, propriedade ou colocação em circulação de qualquer dispositivo eletrónico ou tecnologia que sirva esses efeitos.

2.- Crimes de natureza económica. A Convenção de Budapeste reclama uma proteção adequada dos interesses patrimoniais dos cidadãos através da criação de normas penais que regulem os crimes de falsidade documental e de burla. Se há algo que caracteriza a tecnologia é a possibilidade de que o seu uso fraudulento provoque prejuízos patrimoniais a terceiros sem a necessidade de uma comuni-

cação intersubjetiva, como a exigida de um modo clássico no crime comum de burla. De forma similar, a função de garantia do documento em papel pode não ser cumprida no âmbito tecnológico, pelo que são necessárias normas de novo cunho que regulem a possibilidade de considerar os documentos relevantes jurídico-penalmente a elementos tecnológicos em que o nexo entre documento e criador nem sempre seja possível. A isso se dedicam os artigos 7 e 8 a) e b) da Convenção.

A União Europeia, por seu lado, somou-se à petição dos Estados-Membros para a criação de tipos de infrações penais relativos às fraudes tecnológicas e às falsidades documentais informáticas através da Decisão-Quadro 2001/413/JAI, do Conselho, relativa ao combate contra a fraude e falsificação de meios de pagamento colaterais não monetários, cujo artigo 3 deveria ter servido de referência aos legisladores dos Estados-Membros para a correta absorção dos comportamentos fraudulentos que, como o *phishing* bancário, combinam a tecnologia e a engenharia social para causar prejuízos económicos.

3.- Conteúdos ilícitos. Dois grandes blocos são objeto de atenção por parte da Convenção, do Conselho da Europa e da União Europeia: crimes contra a propriedade intelectual e contra a liberdade sexual. Analisemos ambos separadamente:

a) Crimes contra a propriedade intelectual. Se parte havia que, já nos finais da década dos anos 90 do século passado, estava potencialmente danificada pela sociedade de informação essa era a propriedade intelectual de autores e produtores. O "caso Napster", desencadeado no dealbar da tecnologia *peer to peer*, fez soar o alarme sobre a eficácia real dos clássicos conceitos de comunicação pública ou reprodução como matrizes de tutela dos direitos de autor; anos mais tarde, os sites de torrents poriam em cheque toda a comunidade audiovisual, ao revelar-se como a tecnologia de acesso à obra audiovisual mais nociva da história.

Com vista a uma tutela da propriedade intelectual o mais ampla possível, a proposta original do Conselho Europeu consistiu em fazer "tábula rasa": os Estados-Membros do Conselho deveriam tutelar penalmente todas as infrações de propriedade intelectual derivadas das obrigações assumidas na Acta de Paris, na Convenção de Berna e nos Tratados da OMPI ratificados pelos países assinantes. A referida pretensão, à partida desprovida de qualquer reflexão político-criminal, manteve a redação definitiva da Convenção, embora com a opção de estabelecer reserva, sempre que se garantisse uma tutela satisfatória através de outros meios jurídicos[9]. A União Europeia, por seu lado, enfrentou a era da sociedade de informação através da Diretiva 2001729/CE do Parlamento e do Conselho, relativa à harmonização de determinados aspetos dos direitos de autor e direitos afins aos direitos de autor na sociedade de informação. Através da Diretiva aumentava-se o alcance dos conceitos de comunicação pública e reprodução, a fim de abranger a extensão dos novos desafios para a propriedade intelectual gerados pelas novas tecnologias. A propósito dos denominados sites de torrents, a sentença do TJUE de 13 de fevereiro de 2014 ("Caso *Svenson*"), teve de travar a interpretação expansiva de um conceito, o de comunicação pública, já de si extraordinariamente aberto, fazendo uma interpretação autêntica do que deve ser entendido como tal, sem ultrapassar o artigo 3 da Diretiva[10]. A Diretiva, adicionalmente, originou a obrigação de criação de tipos de infrações penais que antecipassem a tutela da propriedade intelectual até aos mecanismos tecnológicos de proteção da própria propriedade intelectual, sugerindo a sanção penal do fabrico, colocação em circulação, ou evasão de qualquer medida tecnológica tendente à proteção dos direitos de autor. Uma antecipação da tutela que, sem dúvida, supôs a criação de um novo bem jurídico exterior aos direitos de exploração da obra.

b) Crimes contra a liberdade sexual. A constatação do aumento da difusão de pornografia infantil nas redes telemáticas foi o motor de uma política criminal muito expansiva. O aumento da difusão telemática, na realidade, originou um grave problema de discriminação das condutas mais graves que podem ocorrer neste âmbito, com objeto de sancionar penalmente as de maior caráter lesivo, deixando de fora do Direito penal o restante. Na base neste aumento da difusão da pornografia através de novas tecnologias e, especialmente, da Internet, radica, pois, a causa pela qual tantas instituições internacionais, como as de caráter nacional, elaboraram projetos normativos alarmantemente expansivos sobre esta matéria.

Neste contexto não se fala de pornografia entre adultos, mas de pornografia em que figuram meno-

9 Vid. artigo 10 da Convenção.

10 Amplamente sobre esta resolução, contexto e alcance, DE LA IGLESIA ANDRÉS, M., "Comentario a la sentencia del Tribunal de Justicia de la Unión Europea en el caso Svensson: sobre la naturaleza jurídica de los enlaces a obras protegidas por derechos de autor", *Actualidad Jurídica Uría Menéndez (AJUM)*, n.º 37, 2014, pp. 123 e ss.

res. A Convenção, dadas as dificuldades para a punição de algumas das condutas de maior potencial lesivo e dado que não contém normas penais, mas apenas «recomendações» para os Estados que integrem normas penais no seu ordenamento interno, adotou uma proposta amplíssima sobre a matéria, em toda a sua dimensão: conceito de pornografia e situações que a constituem, assim como condutas relacionadas[11]. A maioridade penal é estabelecida nos 18 anos, sancionando-se quaisquer condutas de posse, distribuição, produção ou reprodução de imagens de sexualidade explícita entre ou com menores da referida idade ou inclusivamente com maiores de 18 que simulem ser menores. A participação dos Estados Unidos na Convenção, país em que a liberdade de expressão adquire proporções mais amplas que no território europeu, está na base da possibilidade de estabelecer reserva à punição de condutas relativas à conhecida como pornografia virtual: aquela em que aparecem imagens realísticas de menores que, na verdade, não existem.

A tutela da integridade sexual de menores protagonizada pelo Conselho da Europa não morre com a Convenção da Budapeste. A exploração sexual de menores e o referido fenómeno associado às tecnologias de informação foi objeto de atenção na Convenção de Lanzarote de 25 de outubro de 2007, para a proteção das crianças contra a exploração e o abuso sexual, nos quais se reunia, talvez pela primeira vez de um modo sistemático e articulado, as propostas de punição do denominado *child grooming*, assim como o regime de exceções à distribuição de imagens de sexualidade explícita efetuada pelos próprios menores que participam numa relação sexual.

A União Europeia não se ficou atrás do Conselho da Europa. As primeiras análises da União sobre a matéria foram consagradas na Decisão do Conselho de 29 de maio de 2000 relativa à luta contra a pornografia infantil na Internet (2000/375/JAI). Esta decisão seria pouco depois desenvolvida através da Decisão-Quadro 2004/68/JAI do Conselho, de 22 de dezembro de 2003, relativa à luta contra a exploração sexual de crianças e pornografia infantil, que seguiu a via aberta pela Convenção de Budapeste. A Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra os abusos sexuais e a exploração sexual de menores e pornografia infantil, veio substituir a Decisão-Quadro citada, ampliando o âmbito de intervenção e incluindo, de igual forma, as condutas de *child grooming* (e as suas exceções) desenvolvidas na Convenção de Lanzarote.

Este é, em suma, o alcance das normas supranacionais nesta matéria de criminalidade informática que se tem vindo a desenvolver nos últimos quinze anos. O modo como estes blocos normativos são transpostos para os ordenamentos nacionais pode, sem dúvida, condicionar a sua eficácia.

2 · O MODELO DE TRANSPOSIÇÃO DO DIREITO PENAL PORTUGUÊS

Portugal adotou um modelo tendencialmente "agregado" de transposição da regulamentação internacional sobre esta matéria e agrupou num conjunto normativo específico as regras fundamentais relativas à criminalidade informática – a Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro). Esta lei transpôs para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, respeitante a ataques contra sistemas de informação e adaptou – 8 anos depois - o direito nacional à Convenção de Budapeste, estabelecendo "*as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico* (…)" (Artigo 1.º "Objeto").

A Lei do Cibercrime não foi propriamente uma novidade no ordenamento jurídico português no que respeita à existência de uma lei específica relativa a este tipo de criminalidade, na medida em que desde 1991 já vigorava em Portugal a "Lei da Criminalidade Informática" (Lei n.º 109/91, de 17 de Agosto). Apesar de ter revogado esta legislação, a Lei do Cibercrime herdou parte relevante do que aquela já estabelecia, embora adaptando-se à regulamentação internacional.

Esta opção de "condensação" do legislador português foi fundamentada na Exposição dos Motivos da Proposta de Lei n.º 289/X/4ª por se afigurar ser, por um lado, "*a opção legislativa mais coerente com a tradição portuguesa, onde existe, especificamente na área penal, outros diplomas estruturantes de matérias na especialidade* (…)" e, por outro, em relação às regras processuais, "*a geral inconveniência de ver em diplomas estruturantes do ordenamento penal regras especiais, apenas aplicáveis a uma parcela muito restri-*

11 Vid. artigo 9 da Convenção.

ta dos tipos de ilícito" e "*a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector específico de criminalidade*."

A existência de uma lei especial para a matéria da cibercriminalidade pode, em teoria, facilitar a sua compreensão, coerência e eficácia. No entanto, apesar das aludidas vantagens, não deixaram de se colocar algumas dúvidas interpretativas e pontos de choque no que respeita à sua conciliação com a lei geral, nomeadamente, por exemplo, em questões processuais face à aplicação extensiva desta lei em matéria de obtenção de prova digital (artigo 11.º da Lei do Cibercrime). Além disso, na sociedade atual, dificilmente se pode sustentar que estejamos perante um "setor específico de criminalidade", na medida em que o uso da tecnologia estendeu-se aos mais diversos tipos de criminalidade, nomeadamente a altamente organizada e complexa.

Ainda assim, não há uma "agregação total" numa lei específica, na medida em que, por um lado, não se encontram contemplados na Lei de Cibercrime, mas sim no Código Penal, alguns tipos legais de "crimes informáticos" (pelo menos em parte), como a "Violação de correspondência e telecomunicações" (Artigo 194.º), a "Devassa por meio de informática" (Artigo 193.º), a "Burla Informática e nas comunicações" (Artigo 221.º) e a "Pornografia de menores" (Artigo 176.º) e, por outro, o modelo processual da Lei do Cibercrime mantém uma relação estreita com o modelo processual do Código de Processo Penal.

Através do Decreto-Lei n.º 69/2014, o Governo aprovou uma alteração à Orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (CNCS)[12] cuja missão é "*contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional*" (artigo 2.º, n.º 2).

O CNCS possui competências específicas que desempenha no quadro da Estratégia Nacional de Segurança no Ciberespaço (aprovada pela Resolução n.º 36/2015 do Conselho de Ministros[13]). Esta estratégia assenta em seis Eixos de intervenção: Estrutura e segurança do ciberespaço; combate ao cibercrime; proteção do ciberespaço e das infraestruturas; Educação, sensibilização e prevenção; Investigação e desenvolvimento; Cooperação. Além disso, esta Resolução definiu concretamente as competências do CNCS.

No que respeita especificamente ao combate ao cibercrime, esta Resolução assumiu como medidas a adotar a revisão e atualização da legislação e a agilização das capacidades da Polícia Judiciária. No contexto do compromisso assumido pela Resolução, o Decreto-Lei n.º 81/2016, de 28 de novembro, criou no seio da Polícia Judiciária a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T). Esta unidade, inspirada no modelo adotado pelo EC3 (*European Cybercrime Center*) da EUROPOL tem amplas competências de investigação e combate a este tipo de criminalidade. Além disso, esta unidade assegura o ponto de contacto permanente em matéria de cooperação internacional, nos termos previstos no Artigo 21.º, da Lei do Cibercrime.

Assim, parece evidente que, pelo menos do ponto de vista da atividade legislativa e da criação de mecanismos que a promovam e punam a sua violação, há muito que a segurança do ciberespaço (nas suas diferentes componentes, incluindo a punitiva) tem-se revelado uma preocupação em Portugal. E é algo que se compreende, na medida em que segundo o Relatório Anual de Segurança Interna de 2017[14], há vários anos que se assiste a uma tendência de subida na generalidade destes crimes.

A Lei do Cibercrime é o diploma fundamental respeitante a este tipo de criminalidade. No essencial, a Lei do Cibercrime assume a estrutura da Convenção de Budapeste, dividindo-se em 4 capítulos: (i) Objeto e Definições; (ii) Disposições Penais Materiais; (iii) Disposições Processuais; (iv) Cooperação Internacional.

Abordaremos neste artigo alguns temas respeitantes às "Disposições Penais Materiais" e às "Disposições Processuais".

2.1 · Crimes contra a integridade dos sistemas

Dentro desta categoria de crimes, a Lei do Cibercrime prevê os crimes de "Falsidade informática"

12 https://www.cncs.gov.pt/

13 https://dre.pt/application/conteudo/67468089

14 Vide páginas 31 e 32 em https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6

(Artigo 3.º), Dano relativo a programas ou outros dados informáticos" (Artigo 4.º), "Sabotagem informática" (Artigo 5.º), Acesso ilegítimo (Artigo 6.º), Interceção ilegítima (Artigo 7.º).

Apesar de se dizer que o mundo da tecnologia está em constante evolução (e, de facto, está), no que respeita às disposições penais materiais, não deixa de ser curioso que a Lei do Cibercrime seja uma mera adaptação aos princípios da Convenção de Budapeste do que já estava previsto numa lei de 1991 (a anterior Lei da Criminalidade Informática). Ou seja, é evidente que pelo menos desde os anos 90 já existia em Portugal uma consciência jurídica e uma preocupação legislativa específica de acompanhar a evolução tecnológica e informática, na sua vertente delituosa. Em termos substantivos, é escasso o caráter inovador. Regra geral, no que respeita a estes crimes mantêm-se os elementos objetivos do tipo.

Como questões inovadoras mais relevantes, de harmonia com a Convenção e com o crescente desenvolvimento do comércio associado a estes ilícitos, podemos salientar a inclusão nestes crimes da punição das atividades comerciais relacionadas: importação, venda, distribuição de dispositivos próprios para a consumação destes crimes passaram a constar expressamente destas previsões legais.

Neste campo, não podemos deixar de questionar a redação respeitante ao crime de Falsidade Informática: "*Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações previstas no n.º2*[15] …" (Artigo 3.º, n.º 4 LC). Esta alteração parece visar uma adaptação ao ordenamento português do artigo 6.º, n.º 1, alíneas a) e b), da Convenção do Cibercrime. No entanto, conforme refere Pedro Dias Venâncio "*Da estranha redação "sobre o qual tenha sido praticado", inclusa na parte final deste n.º 4, parece resultar que neste caso o crime só se consuma se o dispositivo vier a ser utilizado. O que contraria toda a lógica da previsão da CCiber que consagra um verdadeiro crime de perigo*." (in Lei do Cibercrime – Anotada e Comentada, Coimbra Editora, 2011, página 40).

Além disso, a Lei do Cibercrime procurou tornar alguns destes tipos mais abrangentes e de prova mais simples. Tal é notório na previsão do Crime de "*Dano relativo a programas ou outros dados informáticos*" ao eliminar-se a anterior exigência da Lei da Criminalidade Informática de existência de intenção do agente de "*causar prejuízo e outrem ou de obter benefício ilegítimo para si ou para terceiros*." O mesmo espírito encontra-se presente na eliminação do elemento subjetivo anteriormente existente no crime de "Sabotagem informática" e no crime de "Acesso Ilegítimo".

2.2 · Crimes de natureza económica

Desde a revisão do Código Penal de 1995 (Decreto-Lei n.º 48/95, de 15 de Março) que está expressamente previsto na legislação penal portuguesa o crime de Burla informática (Artigo 221.º, do Código Penal). Assim, Portugal não teve que adotar nenhuma iniciativa legislativa no sentido de criminalizar a Burla Informática nos termos constantes do Artigo 8.º da Convenção sobre o Cibercrime.

"Trata-se de um crime doloso, de execução vinculada, cometido por interferência no resultado de tratamento de dados de programa informático, quer mediante estruturação incorreta do programa informático quer por utilização incorreta ou incompleta de dados informáticos. A lei alarga ainda a incriminação a dois tipos de procedimentos abusivos, o da utilização de dados informáticos sem autorização, e a intervenção por qualquer outro modo não autorizado no processamento" (In Código Penal – Parte Geral e Especial, Edições Almedina, 2014, página 936). É um crime de resultado, exigindo-se que o agente cause um prejuízo a outrem e tenha uma intenção de enriquecimento ilegítimo para si ou terceiro. Tal circunstância, à semelhança do que acontece com o crime de burla, torna por vezes difícil a prova do crime.

Um dos exemplos mais frequentes considerados pela Jurisprudência Portuguesa como crime de burla informática é a utilização ilegítima de cartões bancários, na medida em que supõe uma "utilização não autorizada de dados."[16]

15 As ações relativas a "dados registados ou incorporados num cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado."

16 Por exemplo: Acórdão da Relação de Évora de 29 de Novembro de 2016; Acórdão da Relação do Porto de 5 de Junho de 2013 (disponíveis em www.dgsi.pt)

2.3 · Crimes contra a propriedade intelectual

À semelhança do que também já sucedia com a revogada Lei da Criminalidade Informática, a Lei do Cibercrime prevê o crime de "Reprodução ilegítima de programa protegido" (Artigo 8.º). Aliás, são de mero detalhe as diferenças entre a previsão anterior e a atual.

Fruto de uma certa "vulgarização" pela comunidade deste tipo de práticas no que respeita, por exemplo, aos mais variados programas de computador, mas também pela importância do bem jurídico protegido, este crime é tem produzido abundante Jurisprudência (ainda que grande parte se refira à anterior Lei da Criminalidade Informática). É pacífico o entendimento de que os elementos típicos do crime ("reprodução", "divulgação" e "comunicação ao público") não são cumulativos, bastando-se para a prática do crime a verificação de apenas um. Ou seja, por exemplo, a mera instalação não autorizada de um programa informático protegido por direitos de autor é suficiente para a prática do crime, não se exigindo qualquer divulgação ou mesmo prejuízo ou lucro. Além disso, é um crime público que não depende de queixa e a tentativa é punível.

Tem sido objeto de debate a razão para o legislador ter sentido necessidade de criar uma previsão específica para os programas de computador. Na verdade, o Código do Direito de Autor e dos Direitos Conexos (Decreto-Lei n.º 63/85, de 14 de Março) já previa um conjunto de crimes relativos à proteção dos direitos de autor ("usurpação", "contrafação", "violação do direito moral", "aproveitamento de obra contrafeita ou usurpada") que, devidamente interpretados, poderiam aplicar-se aos programas informáticos. A verdade é que o legislador português optou por uma visão mais estrita de "obra" e entendeu manter na Lei do Cibercrime uma previsão legal específica para a informática que já existia na anterior Lei da Criminalidade Informática.

2.4 · Pornografia de menores

O crime de "Pornografia de menores" (Artigo 176.º, do Código Penal) está previsto no ordenamento português desde a alteração do Código Penal de 2007 e visou incluir na legislação nacional as diretrizes da Decisão-Quadro do Conselho 2004/68/JAI relativa à luta contra o abuso sexual de crianças, a exploração sexual de crianças e a pornografia infantil. A atual versão incorpora também a trigésima nona alteração ao Código Penal de 2015 (Lei n.º 103/2015, de 24 de Agosto) que transpôs a Diretiva 2011/93/EU, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011.

A previsão criminal assumida pela lei penal portuguesa é abrangente e contempla todas as variantes previstas na Convenção de Budapeste com vista à proteção de menores quanto a este tipo de abusos: desde a utilização de menor em espetáculos, filmes, fotografias ou gravações de cariz pornográfico ou o seu aliciamento para esse fim, passando pelas atividades comerciais relacionadas (produção, distribuição, importação, exportação, exibição ou cedência) até à "mera" detenção e consumo deste tipo de materiais, incluindo através de sistemas informáticos. Além disso, abrange também as "representações realistas" de menores inexistentes.

Assim, quanto a esta matéria, a opção do legislador português foi incluir no Código Penal todas as variantes associadas à pornografia infantil, incluindo obviamente a informática.

Seja como for, assiste-se a alguns debates interpretativos interessantes. Embora não se discutindo que fazer *download* de pornografia de menores constitui crime, não é pacífico na Jurisprudência se tal se enquadra no conceito de "aquisição" e "detenção" (Artigo 176.º, n.º 4, alínea d), do Código Penal) ou de "importação" (Artigo 176.º, n.º 1, alínea c), do Código Penal)[17].

2.5 · Disposições processuais

A grande novidade que Lei do Cibercrime trouxe para o ordenamento português em relação à sua precedente Lei da Criminalidade Informática foi precisamente no campo processual. Na verdade, antes da adaptação do direito interno à Convenção de Budapeste, os crimes de natureza informática seguiam o regime geral do Código de Processo Penal, procurando adaptar-se os modelos de aquisição de prova "tradicionais" a esta realidade. Com intuito de dotar de maior eficácia o combate à criminalidade (não só a especificamente informática), a Lei do Cibercrime veio, pela primeira vez, prever um regime jurídico específico de obtenção de prova digital, estabelecendo no ordenamento português normas relativamente à preservação, revelação, acesso, pesquisa e apreensão de dados informáti-

17 Sobre esta matéria Vide Acórdãos do Tribunal da Relação de Lisboa de 03-12-2014 e de 15-12-2015 (disponíveis em www.dgsi.pt)

cos; apreensão de correio eletrónico e registos de comunicações de natureza semelhante; interceção de comunicações; ações encobertas[18]. O modelo processual da Lei do Cibercrime tem a particularidade de se aplicar não apenas aos crimes previstos nesta lei ou cometidos através de sistema informático, mas também "*Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico*" (Artigo 11.º, n.º 1, alínea c)). Ou seja, a curiosidade desta disposição reside no facto de uma lei processual especial ter aplicação geral, salvo raras exceções. E estas exceções são os meios considerados mais intrusivos, a "Interceção de comunicações" (Artigo 18.º) e as "Ações encobertas" (Artigo 19.º) cuja aplicação segue, no primeiro caso, o regime de admissibilidade geral previsto para as escutas telefónicas no artigo 187.º, do Código de Processo Penal (por exemplo, crimes puníveis com pena de prisão superior a 3 anos, tráfico de estupefacientes, contrabando, terrorismo, criminalidade violenta e altamente organizada, etc.) e, no segundo caso, um conjunto de crimes cometidos por meio de um sistema informático, nos termos da alínea a), do n.º 1, do Artigo 19.º da Lei do Cibercrime (como por exemplo, crimes com penas de prisão máxima superior a 5 anos, crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, infrações económico-financeiras, crimes relativos a direitos de autor, etc.).

É neste capítulo processual que se têm gerado maiores dificuldades resultantes do modelo de transposição português "agregado" na Lei do Cibercrime em comparação com um modelo que procedesse à revisão integrada do processo penal para inclusão de um regime processual mais adequado à generalização dos meios informáticos na vida em sociedade. Na verdade, exige-se uma convivência conjunta do processo penal geral com este nascido com a Lei do Cibercrime e que, por vezes, gera algumas dificuldades adicionais que poderiam ter sido evitadas. Desde logo, seguindo uma, salvo melhor opinião, questionável tradição legislativa portuguesa, existem várias remissões nesta lei para o Código de Processo Penal (com as devidas adaptações)[19]. Além disso, este regime específico quanto à obtenção de prova digital não significa que outros não mantenham plena pertinência no "digital", como por exemplo, a prova pericial (artigos 151.º e seguintes do Código de Processo Penal). Mas, mais exemplificativo, é o facto de a Lei do Cibercrime não ter revogado expressamente a "Extensão" do regime das escutas telefónicas às comunicações eletrónicas, constante do artigo 189.º, do Código de Processo Penal. Ou seja, pelo menos aparentemente, parte relevante da mesma realidade poderia estar regulada por disposições legais distintas.

Sem prejuízo de ser questionável a opção de não incluir no Código de Processo Penal o regime processual relativo à obtenção de prova digital, é cada vez mais pacífico na Jurisprudência que o regime processual das comunicações telefónicas (artigos 187.º a 190.º, do Código de Processo Penal) "*deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.*"[20]. Conforme sustenta Paulo Dá Mesquita, o "Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal" (In "Processo Penal, Prova e Sistema Judiciário, Wolters Kluwer/Coimbra Editora, 2010, página 101).

Em conclusão, independentemente das vantagens e desvantagens que qualquer modelo interno de transposição da regulamentação internacional em matéria de Cibercrime tem, Portugal tem sido do ponto de vista legislativo um "bom aluno", contemplando no seu ordenamento jurídico a generalidade das diretrizes internacionais nesta matéria. Portanto, a maior ou menor eficácia do combate ao Cibercrime em Portugal não parece estar tão dependente da bondade das leis, mas sim do investimento e organização dos meios humanos e tecnológicos que um país ainda a recuperar de uma crise económica recente tem conseguido alocar para esse efeito.

3 · O MODELO DE TRANSPOSIÇÃO DO DIREITO PENAL ESPANHOL

A abordagem abrangente da Convenção de Cibercriminalidade teria permitido criar no nosso país um bloco legislativo consistente e coerente com este âmbito concreto, como sucede em Itália ou em

18 Artigos 11.º a 19.º da Lei do Cibercrime

19 Como por exemplo os Artigos 14, n.º 7, 15.º, n.º 6, 16.º, n.ºs 5 e 6, 17.º, 18.º, n. 1, a) e 4

20 Acórdão do Tribunal da Relação de Évora de 20-01-2015

Portugal. A exigência da lei orgânica para regular matérias que afetem direitos fundamentais e liberdades públicas, que exige maiorias parlamentares reforçadas com os consequentes custos em termos de tempo, esforço e consenso político certamente dificultou esta possibilidade. Igualmente, o facto de a Convenção de Budapeste não ter sido ratificada pelo Reino Unido até 20 de maio de 2010, muito provavelmente atuou como travão. Nesse lapso temporal foram surgindo diversas iniciativas de harmonização legislativa relativa à cibercriminalidade no âmbito da União Europeia. Apesar de que isso não teria constituído impedimento para uma visão de conjunto da matéria no nosso Código, as adaptações do ordenamento jurídico espanhol em algumas das matérias próprias da Convenção, durante o período que foi de 2001 a 2010, foram realizadas de forma progressiva e desarticulada, ao ritmo da transposição ou inclusão das correspondentes Diretivas ou Decisões-Quadro comunitárias mencionadas na primeira parte do presente artigo. Entram neste período de pré-ratificação da Convenção as reformas efetuadas no Código Penal pelas Leis Orgânicas de 15/2003, de 25 de novembro e 5/2010, de 22 de junho, assim como a promulgação da Lei 25/2007, de 18 de outubro, de conservação de dados relativos às comunicações eletrónicas e às redes públicas de comunicações.

A ratificação da Convenção abriu uma nova fase de reformas legislativas em Espanha que teve maior impulso devido à Diretiva 2013/40/UE, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de informação. Neste período enquadra-se a reforma do Código Penal operada pela Lei Orgânica 1/2015, de 30 de março, e a reforma da Lei do Processo Penal no âmbito das medidas de investigação tecnológica operada pela Lei Orgânica 13/2015, de 5 de outubro. De igual forma, a citada Diretiva 2013/40/UE veio concretizar o impulso prévio da União Europeia no sentido de uma política comum de cibersegurança e a sua transposição para os diferentes Estados-Membros, o que se traduziu na adoção por Espanha de uma Estratégia de Cibersegurança Nacional[21] no final de 2013 e um acompanhamento específico dos dados estatísticos da cibercriminalidade por parte do Ministério do Interior também desde 2013. Por último, a mais recente Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa às medidas destinadas a garantir um elevado nível comum de segurança das redes e sistemas de informação na União, deu mais um passo na política comum de cibersegurança encaminhado para a proteção dos serviços essenciais e as infraestruturas críticas estatais dependentes de redes e sistemas de informação.

Esta fragmentação da legislação penal provocará, como se verá em seguida, acentuadas dissonâncias entre a pretensão real do legislador e a *mens legis*, que em muitos casos obrigam a desvirtuar os bens jurídicos gerais dos títulos e capítulos em que se inscrevem as novas figuras típicas para conferir um sentido razoável ao seu resultado.

3.1 · Crimes contra a integridade dos sistemas (hacking e danos informáticos)

A inclusão no ordenamento espanhol de crimes relativos à integridade dos sistemas sobre a base das condutas de intrusão ou interceção ilegal (*hacking*) e causalidade de resultados danosos ou sabotagem (danos informáticos) requereu duas reformas legislativas do Código Penal.

Num momento inicial, estas figuras penais foram introduzidas por meio da Lei Orgânica 5/2010, de 22 de junho[22], com base nas diretrizes estabelecidas pela Decisão-Quadro 2005/222/JAI. A primeira criminalização[23] do *hacking* em Espanha ficou concretizada no aditamento do n.º 3 no artigo 197 do CP que penaliza os crimes contra a privacidade e o sigilo das comunicações. Trata-se de uma criminalização limitada dos acessos ilícitos em comparação com a proposta da Convenção de Budapeste, pois requeria, além da ausência de autorização, a viola-

21 O documento de Estratégia de Cibersegurança Nacional espanhola pode ser consultado no seguinte link: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

22 Para uma análise em profundidade da reforma penal de 2010 nestas matérias vid. MORALES GARCÍA, Oscar, *Delincuencia informática. Intrusismo, sabotaje informático y uso ilícito de tarjetas, arts. 197.3 e 8, 264 e 248 CP*. Em La reforma penal de 2010. Análisis y contenido. Ed. Aranzadi (Cizur Menor) 2010; HURTADO ADRIÁN, Ángel Luis, *Accesos informáticos ilícitos (art. 197 apdo. 3)*. Em Reforma del Código Penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Ed. El Derecho (Madrid) 2010; e DE LA MATA BARRANCO, Norberto Javier, *El delito de daños a datos, programas, documentos y sistemas informáticos*. Em Reforma del Código Penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Ed. El Derecho (Madrid) 2010.

23 Sobre a penalização das condutas de *hacking* antes da reforma penal de 2010 vid. MOLINA GIMENO, Francisco Javier, *El hacking, ¿una conducta punible?*. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 7131. Ano 2009.

ção de medidas de segurança e que a intrusão afetasse dados ou programas informáticos constantes no sistema em questão. De igual forma, a sua integração no artigo 197 fazia com que partilhasse o bem jurídico vinculado com a privacidade própria das condutas contidas nessa disposição, o que, na prática, dificultava a sua aplicação ao exigir do sujeito ativo da intrusão uma vontade de violar a privacidade de terceiros. O crime de danos informáticos, por seu lado, foi incluído em 2010 como disposição penal específica no artigo 264 do CP, que incluía um primeiro parágrafo relativo à afetação de programas ou documentos informáticos por meio de apagamento, deterioração, alteração ou supressão e um segundo parágrafo relativo à obstaculização ou interrupção do funcionamento de um sistema. Ambas as modalidades coincidiam substancialmente com as disposições dos artigos 4 (interferência nos dados) e 5 (interferência no sistema) da Convenção de Budapeste. No entanto, o legislador espanhol limitou o alcance das referidas infrações acrescentando os requisitos de ser necessária uma ação por parte de outrem em relação aos dados ou ao sistema afetado e da gravidade tanto da ação em si mesma (desvalorização reforçada da conduta) como dos danos finalmente produzidos (desvalorização reforçada do resultado). Em ambos os grupos de crimes foi introduzida a responsabilidade penal da pessoa coletiva.

A posterior transposição da Diretiva 2013/40/UE por meio da reforma do Código Penal operada pela Lei Orgânica 1/2015, de 30 de março, situou a criminalização penal espanhola do *hacking* e dos danos informáticos[24] nos termos propostos pela Convenção de Budapeste. No respeitante ao *hacking*, a reforma de 2015 criou uma disposição específica, o artigo 197 bis, que nos seus parágrafos contém, por um lado, a regulamentação das condutas de acesso ilícito e não consentido, violando medidas de segurança (artigo 2.º da Convenção), relativa, desta vez, aos sistemas em si mesmos e já não aos dados ou programas nestes constantes e, por outro lado, as condutas de intercetação ilícita de transmissões de dados em sistemas de informação, incluindo as emissões eletromagnéticas (artigo 3.º da Convenção). Esta nova criminalização autónoma permite identificar, num bem jurídico protegido próprio, a integridade dos sistemas, desvinculado o direito à privacidade dos utilizadores, e facilitando assim a sua persecução. No âmbito dos danos informáticos, a reforma de 2015, sem que se alterasse na essência a criminalização básica introduzida em 2010, dividiu as condutas de danos em duas disposições: por um lado, o artigo 264 do CP criminaliza agora unicamente as condutas de afetação danosa dos dados, programas ou documentos por meio de apagamento, deterioração, alteração ou supressão (interferência nos dados); por outro lado, o novo artigo 264 bis do CP penaliza as condutas de obstaculização ou interrupção do funcionamento de sistemas (interferência no sistema). Ambas as classificações continuam a exigir uma ação por parte de outrem em relação aos dados, programas ou sistemas objeto do ataque (o que levanta dificuldades interpretativas para perseguir ações prejudiciais realizadas por utilizadores registados contra o seu próprio sistema) e um elemento de gravidade na conduta e no resultado (cuja indeterminação concetual também pressupõe dificuldades interpretativas e probatórias na prática). Talvez a novidade mais relevante neste âmbito resida nas novas circunstâncias agravantes específicas introduzidas pela reforma para ambas as modalidades de danos informáticos (parágrafos 2 e 3 dos artigos 264 e 264 bis), podendo as penas atingir os oito anos de prisão. Nesta bateria de agravantes, destaca-se o compromisso político-criminal comunitário na luta contra a cibercriminalidade, que se materializa em fenómenos como os ciberataques massivos, o uso de *ransomware* ou o roubo de identidade (*identity theft*).

Por último, a reforma de 2015 também incluiu no ordenamento espanhol a criminalização autónoma do abuso de dispositivos (artigo 6 da Convenção) por meio de duas disposições, os novos artigos 197 ter e 264 ter do CP que penalizam a produção, aquisição, importação ou distribuição sem autorização de programas ou dados (por ex. palavras-passe ou códigos) especificamente destinados à prática de crimes de *hacking* ou de danos informáticos, respetivamente. Desta forma fechou-se uma tipificação

24 Para uma análise em profundidade desta reforma legislativa consultar a Circular 3/2017 da Fiscalía General del Estado sobre a reforma operada pela LO 1/2015 de 30 de março relativa aos crimes de descoberta e divulgação de segredos e os crimes de danos informáticos. No mesmo sentido, MORALES PRATS, Fermín, *La reforma de los delitos contra la intimidad artículo 197 CP.* Em *Comentario a la reforma penal de 2015*. Ed. Aranzadi (Cizur Menor) 2015; ANDRÉS DOMINGUEZ, Ana Cristina, *Reformas en daños*. Em Comentario a la reforma penal de 2015. Ed. Aranzadi (Cizur Menor) 2015; COLÁS TURÉGANO, Asunción, *Nuevas conductas delictivas contra la intimidad (arts. 197, 197 bis e 197 ter)*. Em Comentarios a la reforma del Código Penal de 2015. Ed. Tirant lo Blanch (Valencia) 2015; GUINARTE CABADA, Gumersindo e CASTRO CORREDOIRA, María, *La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quater, 265, 266.1 e 266.2 CP*. Em Comentarios a la reforma del Código Penal de 2015. Ed. Tirant lo Blanch (Valencia) 2015

que transpõe para o ordenamento espanhol praticamente na íntegra os artigos 2.º a 6.º da Convenção de Budapeste.

3.2 · Crimes de natureza económica (burla informática)

A Convenção e as Diretivas adotam uma abordagem tendente à penalização efetiva de fenómenos de cibercriminalidade largamente difundidos, como o *phishing*, o *pharming*, o *identity theft* e outras condutas equiparáveis.

O legislador espanhol não chegou a incluir uma penalização para a falsidade e a fraude informática nos termos da Convenção de Budapeste, nem sequer nos termos do artigo 3.º da Decisão-Quadro 2001/413/JAI especificamente referente às fraudes informáticas. O atual Código Penal espanhol foi aprovado em 1995 e na sua redação original foram incluídas disposições que viriam a permitir a penalização de documentos eletrónicos falsos e burlas informáticas. Por um lado, o artigo 26.º do CP incluiu uma definição autêntica de documento para efeitos penais muito ampla, inclusiva de suportes informáticos, de documentos eletrónicos e de dados contidos em sistemas[25]como potencial objeto de falsificação. Por outro lado, o crime de burla do artigo 248 do CP foi dotado de uma segunda modalidade típica consistente na obtenção de uma transferência não consentida de qualquer ativo por meio de manipulação informática ou artifício semelhante. Por último, o artigo 400 do CP penalizava com as mesmas penas tanto os autores materiais de crimes de falsificação documental como os fabricantes ou detentores de programas informáticos destinados à realização das referidas falsificações.

A Lei Orgânica 15/2003, de 25 de novembro acrescentou um terceiro parágrafo ao crime de burla do artigo 248 que penalizava o fabrico, posse ou distribuição de programas de computador especificamente destinados à prática de fraude, e a reforma penal de 2010 introduziu uma nova modalidade típica consistente na utilização de cartões de crédito, débito, cheques de viagens ou dados nestes constantes para realizar operações com prejuízo dos titulares[26].

A atual penalização destas condutas no Código Penal espanhol, ainda contando com elementos específicos como a manipulação informática, continua vinculada aos princípios e estruturas interpretativas históricas dos crimes de fraude (por exemplo, engano intersubjetivo, erro de um terceiro, deslocação patrimonial de vítima para autor, alteração de elementos essenciais do documento, etc.) que dificultam a persecução e penalização como crimes patrimoniais[27]de condutas tendentes à obtenção de um benefício ilícito com base na intrusão em sistemas de informação (*phishing* e *pharming*)[28], os ataques de informação *(ransomware)* ou a aplicação ilícita de dados pessoais de terceiros *(identity theft)*.

3.3 · Crimes contra a propriedade intelectual

A reforma penal de 2003 adaptou o artigo 270 do CP à Diretiva 2001/29/CE, cujos conceitos de reprodução, distribuição, comunicação pública, importação e exportação de obras protegidas, eram, sem dúvida, mais amplos do que o contido no Texto Consolidado de Propriedade Intelectual. A criminalização alargou-se a obras fixadas em qualquer tipo de suporte ou comunicadas através de qualquer meio (o que abria a porta às infrações cometidas por meio de tecnologias da informação). Por fim, na linha expansiva da Diretiva, introduziu-se uma penalização específica para o fabrico, posse, importação ou distribuição de meios destinados à supressão não autorizada ou neutralização de medidas técnicas de proteção de programas informáticos, obras, interceções e execuções.

---

25 Nesse sentido, a jurisprudência do Tribunal Supremo conferiu a condição de documento para efeitos penais e, portanto, suscetíveis de falsificação, os suportes informáticos como disquetes ou dispositivos óticos (STS de 2 de dezembro de 2000 [RJ 2000, 9955]), os discos rígidos (STS de 4 de novembro de 2009 [RJ 2009, 7871]), as bases e ficheiros de dados informáticos contidos em sistemas (STS 9 de abril de 2007 [RJ 2007, 4715], STS de 16 de junho de 2014 [RJ 2014, 3451] e STS de 24 de maio de 2017 [RJ 2017, 3305]) e os documentos eletrónicos em todas as suas formas (STS de 19 de maio de 2016 [RJ 2016, 6532]).

26 Sobre a reforma penal de 2010 neste âmbito vid. HURTADO ADRIÁN, Ángel Luis, *Estafa informática (art. 248 apdo. 2).* Em *Reforma del Código Penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio*. Ed. El Derecho (Madrid) 2010.

27 Cfr. a política criminal espanhola nos cibercrimes patrimoniais FARALDO CABANA, Patricia, *Estrategias legislativas en la reformas de los delitos informáticos contra el patrimonio*. Em Revista Aranzadi de Derecho y Nuevas Tecnologías. N.º 42. Ano 2016.

28 Vid., neste sentido, REY HUIDOBRO, Luis Fernando, *La estafa informática: relevancia penal del phishing y el pharming*. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 7926. Ano 2012 e VELASCO NÚÑEZ, Eloy, *Estafa informática y banda organizada. Phishing, pharming, smishing y muleros.* Em La Ley Penal. N.º 49. Ano 2008.

Foi com a reforma penal de 2015[29] que se tentou dar resposta ao aparecimento de novas formas de violação de direitos de propriedade intelectual no contexto da Internet (por exemplo, intercâmbio de arquivos P2P ou *sites* de *torrents* ou de *uploading*) até então de penalização limitada[30]. As novas realidades tecnológicas apresentavam dificuldades de enquadramento em conceitos típicos, como a comunicação pública ou a orientação para o lucro[31]. O legislador reformou dois tipos penais nos seguintes termos:

(i) A modalidade básica do crime inclui uma nova conduta típica aberta consistente em "qualquer outro modo de exploração económica" da obra, o que permite abarcar infrações da propriedade intelectual que possam ocorrer no futuro e que não se enquadrem nos conceitos básicos de reprodução, plágio, distribuição ou comunicação pública. A fórmula aberta aplicada pelo legislador neste caso suscita dúvidas da perspetiva do princípio de taxatividade estabelecida na redação dos tipos penais.

(ii) São incluídos como objeto de proteção de tipo básico as prestações de serviços, definidas como direitos de autor e direitos conexos dos artigos 105 a 128 da Lei de Propriedade Intelectual. Esta ampliação objetiva permite, por exemplo, conceder tutela penal às retransmissões de eventos desportivos de canais pagos (televisão ou *streaming*).

(iii) O elemento típico de orientação para o lucro é substituído pela intenção de "obter um benefício económico direto ou indireto" em todas as modalidades típicas dos crimes contra a propriedade intelectual. A reforma mantém a natureza comercial da intenção de obter benefício e alarga-o aos rendimentos comerciais indiretos (como podem ser os benefícios obtidos por *banners* de publicidade em *sites* de *torrents*).

(iv) Criminaliza-se expressamente a atividade de facilitação de acesso ilícito a conteúdos protegidos na Internet, com especial referência aos *sites* de *torrents* que oferecem listas ordenadas e classificadas de obras. Esta conduta típica requer, tal como a modalidade básica, a ausência da autorização do titular, prejuízo de terceiros e intenção de obter benefício. Apenas serão consideradas criminosas as condutas que consistam em oferecer acesso a esses conteúdos de forma ativa e não neutral e sem se limitar a um tratamento puramente técnico, de modo que se exclui a criminalização de serviços neutrais como os motores de busca da Internet.

(v) Por último, é facultado aos juízes penais faculdade para atuar, cautelarmente e em sentença, sobre os conteúdos ilícitos, ordenando a retirada das obras ou prestações objeto de infração e, caso se aplique, a interrupção do serviço ou o bloqueio da página Web ou aplicação por meio da qual se está a cometer o crime.

3.4 · Pornografia infantil

O crime de pornografia infantil vinculado às tecnologias de informação foi objeto de atenção nas reformas penais de 2003, 2010 e 2015, de modo que progressivamente foram sendo assimiladas no regulamento espanhol as propostas de criminalização expansiva incluídas no artigo 9.º da Convenção de Budapeste (que, por sua vez, foram sendo integradas nos instrumentos de harmonização comunitária neste âmbito).

A Lei Orgânica 15/2003, de 25 de novembro, deu o primeiro passo na assimilação dos postulados da Convenção de Budapeste no respeitante a esta

29 Para uma análise em profundidade desta reforma legislativa consultar a Circular 8/2015 da Fiscalía General del Estado sobre os crimes contra a propriedade intelectual através dos serviços da sociedade de informação após a reforma operada pela Lei Orgânica 1/2015. E também, GALÁN MUÑOZ, Alfonso, La reforma de los delitos contra la propiedad intelectual e industrial. Em Comentario a la reforma penal de 2015. Ed. Aranzadi (Cizur Menor) 2015; TOMÁS-VALIENTE LANUZA, Carmen, *Delitos contra la propiedad intelectual (arts. 270 e 271 CP)*. Em Comentarios a la reforma del Código Penal de 2015. Ed. Tirant lo Blanch (Valencia) 2015; TIRADO ESTRADA, Jesús José, *Los delitos contra la propiedad intelectual tras la reforma del Código Penal de 2015*. Em La propiedad intelectual en la era digital. Ed. Dykinson (Madrid) 2016; e RODRÍGUEZ MORO, Luis, *Las prestaciones: nuevo objeto material en los delitos contra la propiedad intelectual tras la reforma del Código Penal por la LO 1/2015*. Em Actas de Derecho Industrial y Derecho de Autor. N.º 37. Ano 2017.

30 Veja-se nesse sentido a análise realizada por PERALTA GUTIÉRREZ, Alfonso, *Aproximación a los delitos relativos a la propiedad intelectual. Especial referencia a la problemática del intercambio de archivos "Peer to Peer" o P2P*. Em Cuestiones actuales de la propiedad intelectual. Ed. Reus (Madrid), 2010. Na mesma linha vid. GIL GIL, Alicia e MARTÍN FERÁNDEZ, Carlos, *Sobre la tipicidad de la conducta de colgar en la red una obra protegida con ánimo comercial y la atipicidad de su descarga a pesar de su ilicitud*. Indret nº 2/2009.

31 *In extenso*, GARCÍA ALBERO, Ramón, *Las nuevas tecnologías de la información y los delitos contra la propiedad intelectual e industrial en Internet*, *passim*., Editorial de la Universitat Oberta de Catalunya, 2005, particularmente em relação à problemática da orientação para o lucro, analisada pela Fiscalía General del Estado.

infração penal, modificando o artigo 189 do CP[32]. Nesta linha, ampliou-se o alcance das condutas básica de uso de menores para elaborar material pornográfico (incluindo o financiamento de tais atividades) e de produção e distribuição do referido material, qualificou-se a sua posse para uso próprio, assim como, a produção, distribuição ou exibição de material no qual embora não tenham participado efetivamente menores se tivesse incluído a sua voz ou imagem alterada ou modificada.

A reforma penal operada pela Lei Orgânica 5/2010, de 22 de junho, integrou no ordenamento espanhol as diretrizes da Decisão Quadro 2004/68/JAI em matéria de crimes de pornografia infantil[33]. As condutas básicas do artigo 189 do CP foram alargadas à captação de menores para a elaboração de material pornográfico e a obtenção de lucro com tais atividades e foi incluída a responsabilidade penal da pessoa coletiva para estes crimes. Adicionalmente, foi criminalizado pela primeira vez o *child grooming*[34] por meio de um novo artigo 183 bis que penalizava o contacto abusivo com menores de 13 anos através da Internet ou de qualquer outra tecnologia de informação e comunicação com a finalidade de manter relações sexuais ilícitas.

Após a aprovação da Diretiva 2011/93/EU, coube à Lei Orgânica 1/2015, de 30 de março[35], fazer com que os crimes de pornografia infantil tivessem a criminalização de maior alcance na linha proposta pela Convenção de Budapeste de 2001. A reforma integra crimes de posse para o autoconsumo, incluindo imagens de pornografia virtual e de maiores que simulam ser menores, *child grooming* ou *sexting*[36]. Desta forma, aumenta o debate sobre a oportunidade de reformas sobre crime associado às Tecnologias de informação disseminadas pelo CP, pois alguns destes comportamentos, uma vez assumida a necessidade de pena, desvirtuarão os bens jurídicos clássicos (liberdade sexual) até os tornar irreconhecíveis (como entender que a liberdade sexual de um menor é lesada numa imagem de pornografia entre adultos que simulam ser menores ou em imagens realistas de pessoas inexistentes na realidade).

3.5 · A reforma processual de 2015 em matéria de investigação tecnológica

Até ao ano de 2015, a persecução e investigação penal da cibercriminalidade em Espanha regia-se por disposições da Lei do Processo Penal de 1881 que não eram reformadas há décadas (por ex., a regulamentação das intervenções telefónicas, da revisão de documentos, etc.) com as devidas dificuldades práticas e interpretativas que isso implicava[37].

A reforma da LECrim. operada pela LO 13/2015, introduz através dos artigos 588 bis a 588 octies uma extensa e exaustiva regulamentação processual da ciberinvestigação que assume praticamente na íntegra os postulados da Convenção de Budapeste[38].

---

32 Para uma análise em profundidade desta reforma legislativa consultar a Circular 3/2006 da Fiscalía General del Estado sobre determinadas questões relativas aos crimes relacionados com a pornografia infantil. Vid. também GARCÍA VALDES, Carlos, *Acerca del delito de pornografía infantil*. Em Estudios penales en recuerdo del profesor Ruiz Antón. Ed. Tirant lo Blanch (Valencia) 2004.

33 Sobre esta reforma legislativa vid. TAMARIT SUMALLA, Josep María, *Delitos relativos a la pornografía infantil y otras medidas relacionadas con la delincuencia sexual, arts. 189 e 192 CP*. Em La reforma penal de 2010. Análisis y contenido. Ed. Aranzadi (Cizur Menor) 2010 e GARCÍA HERNÁNDEZ, Gema, *Pornografía infantil*. Em El Derecho a la imagen desde todos los puntos de vista. Ed. Aranzadi (Cizur Menor) 2011.

34 Para uma análise detalhada desta nova infração vid. RAMOS VÁZQUEZ, José Antonio, *El llamado delito de child grooming: consideraciones acerca del nuevo artículo 183 bis del Código Penal*. Em El nuevo Código Penal. XXXII Jornadas de la Abogacía General del Estado. Madrid, 17 e 18 de novembro de 2010. Ed. Ministerio de Justicia (Madrid) 2010; MENDOZA CALDERÓN, Silvia, *El fenómeno del acoso a menores "Grooming" desde la perspectiva del Derecho penal español*. Em El acoso: tratamiento penal y procesal. Ed. Tirant lo Blanch (Valencia) 2011; PÉREZ FERRER, Fátima, *El nuevo delito de ciberacoso o child grooming*. La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. N.º 7915. Ano 2012; e GORRIZ ROYO, Elena, *"Online child grooming" en Derecho penal español*. Em Indret. Revista para el Análisis del Derecho. N.º 3. Ano 2016. De igual forma, vid. a STS de 24 de fevereiro de 2015 (RJ 2015, 1405).

35 A Circular 2/2015 da Fiscalía General del Estado analisa em detalhe o alcance da reforma de 2015 nos crimes de pornografia infantil. Neste sentido, vid. ESCUDERO GARCÍA-CALDERÓN, Beatriz, *El delito de pornografía infantil*. Em Comentario a la reforma penal de 2015. Ed. Aranzadi (Cizur Menor) 2015.

36 Para uma análise em pormenor da criminalização do *sexting* vid. RAMOS VÁZQUEZ, José Antonio, *Grooming y sexting: artículo 183 ter CP*. Em Comentarios a la reforma del Código Penal de 2015. Ed. Tirant lo Blanch (Valencia) 2015 e ARNAIZ VIDELLA, Javier, *El sexting en el código penal español*. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8995. Ano 2017.

37 Nesse sentido, vid. VELASCO NÚÑEZ, Eloy, *Aspectos procesales de la investigación y de la defensa en los delitos informáticos.* Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 6506. Ano 2006 e MAGRO SERVET, Vicente, *La instrucción de los delitos informáticos*. Em Estudios de Derecho Judicial. La instrucción de los delitos económicos y contra la hacienda pública. Ed. Consejo General del Poder Judicial (Madrid) 2005.

38 Para uma análise em profundidade da reforma processual de 2015 em matéria tecnológica vid. MARCHENA GÓMEZ, Manuel/GONZÁLEZ-CUELLAR SERRANO, Nicolás, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, 2015; BUENO DE

Aqui cabe destacar que a reforma pretende harmonizar quaisquer questões relativas à intervenção e acesso a comunicações telemáticas, desde os dados das comunicações até aos de conteúdo, dispositivos de armazenamento, captação de voz ou imagem e, em suma, qualquer elemento probatório de natureza tecnológica que possa ser útil para efeitos de investigação.

Dado o impacto nos direitos fundamentais, a LECrim. subordina quaisquer destas medidas ao princípio da especialidade: a investigação deverá ter por objeto o esclarecimento de um facto punível concreto, proibindo-se expressamente investigação prospetiva. E deverão satisfazer os princípios de idoneidade, excecionalidade, necessidade e proporcionalidade, cuja ocorrência deverá estar suficientemente justificada na comunicação judicial para esses efeitos.

Os registos remotos sobre equipamentos informáticos (por ex. por meio do recurso a vírus *trojan* ou *spyware*), em linha com os debates ocorridos entre 1999 e 2001 à volta da Convenção de Budapeste, serão unicamente autorizados para um grupo específico de crimes graves (por ex. terrorismo, traição, etc.) e para qualquer crime cometido através de instrumentos informáticos ou de qualquer tecnologia de informação ou comunicação. A devida comunicação deverá especificar os computadores, dispositivos ou sistemas objetos do registo, o modo de acesso, o *software* a usar, caso se aplique, os agentes intervenientes e as condições de preservação da integridade dos dados. Também se regulam os deveres de colaboração de prestadores de serviços de telecomunicações e sociedade de informação nestes casos. A medida terá uma duração inicial de um mês, prorrogável até três. De igual forma, será obrigatória a conservação de dados ou informações incluídas num determinado sistema informático de armazenamento até que se obtenha a autorização judicial correspondente [39].

Pela primeira vez regula-se também a figura do agente encoberto informático [40] que, também com prévia autorização judicial, pode atuar em canais fechados de comunicação para o intercâmbio ou envio de arquivos ilícitos devido ao seu conteúdo no decurso de uma investigação (por ex., grupos ou fóruns jiadistas ou de intercâmbio de pornografia infantil).

Em conclusão, a fragmentação regulatória em matéria de crimes associados aos processos de transferência de dados, assim como os mecanismos de investigação judicial e cooperação internacional geram riscos para efetiva tutela dos interesses em jogo, assim como uma desvirtuação dos bens jurídicos, afetação do alcance de infrações penais pré-existentes e, sobretudo, o esbatimento da força da mensagem regulamentar que a luta contra a criminalidade informática deveria acarretar.

MATA, Federico, *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.* Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8627. Ano 2015; RUBIO ALAMILLO, Javier, *La informática en la reforma de la Ley de Enjuiciamiento Criminal*. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8662. Ano 2015; CABEZUDO RODRÍGUEZ, Nicolás, *Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal*. Em Nuevos horizontes del Derecho Procesal. Libro homenaje al profesor Ernesto Pedraz Penalva. Ed. Bosch (Barcelona) 2016; JIMÉNEZ SEGADO, Carmelo e PUCHOL AIGUABELLA, Marta, *Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos*. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8676. Ano 2016; CASTILLEJO MANZARES, Raquel, *Alguna de las cuestiones que plantean las diligencias de investigación tecnológica*. Em Revista de Derecho y Proceso Penal. N.º 45. Ano 2017.

39 Esta disposição vem transpor de forma quase literal o artigo 16.º da Convenção de Budapeste sobre conservação expedita de dados informáticos armazenados.

40 Para uma análise detalhada desta nova figura vid. LAFONT NICUESA, Luis, El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal. Em La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8580. Ano 2015; VALIÑO CES, Almudena, *Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015*. Em La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. N.º 8731. Ano 2016 y ZARAGOZA TEJADA, Javier Ignacio, *El agente encubierto online: la última frontera de la investigación penal*. Em Revista Aranzadi Doctrinal. N.º 1. Ano 2017.