CIBERCRIME
e E-EVIDENCE

• COLEÇÃO FORMAÇÃO CONTÍNUA •

• JUNHO 2026 •

• JURISDIÇÃO PENAL E PROCESSUAL PENAL •

CENTRO DE ESTUDOS JUDICIÁRIOS

CEJ

Diretor

Edgar Taborda Lopes, Juiz Desembargador

Diretores Adjuntos

Diogo Ravara, Juiz Desembargador

Fernando Martins Duarte, Juiz Desembargador

Margarida Amadinho da Paz, Procuradora da República

Pedro Raposo de Figueiredo, Juiz Desembargador

Coordenador do Departamento de Relações Internacionais

Valter Batista, *Procurador da República*

FICHA TÉCNICA

Nome

Cibercrime e *e-evidence*

Coleção

Formação contínua

Jurisdição

Penal e Processual Penal

Organização

Jurisdição Penal e Processual Penal

Coordenação

Antero Taveira, *Procurador da República, docente do CEJ*

Intervenientes

Rui Teixeira, *Juiz Desembargador em funções no Tribunal da Relação de Lisboa*

Valter Alves, *Procurador da República em funções na 7.ª Secção do DCIAP*

Antero Taveira

Rui Cardoso, *Procurador-Geral Adjunto, Diretor do DCIAP*

Revisão final

Edgar Taborda Lopes

Notas

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização de um programa leitor de PDF.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Forma de citação de um livro eletrónico (NP405-4)

Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL:
http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

Registo das revisões efetuadas ao e-book	
Identificação da versão	**Data de atualização**
30/06/2026	

Notas iniciais

Preparação, formação, publicação.

É responsabilidade do Centro de Estudos Judiciários contribuir para que os/as magistrados/as portugueses/as disponham de materiais de qualidade que os auxiliem no exercício das suas funções.

Preparada e realizada a acção de formação contínua chega agora o momento da publicação do e-book correspondente, com uma enorme actualidade e antecipando alterações legais que levarão a novas publicações.

Que a todos/as seja útil!

Edgar Taborda Lopes

Há muito que o cibercrime não é uma ameaça emergente, mas uma realidade consolidada. Os dados disponíveis confirmam uma tendência inequívoca: os crimes praticados por meios informáticos ou com recurso a sistemas digitais representam uma fatia crescente da criminalidade participada em Portugal e na União Europeia, com reflexos diretos na atividade das autoridades judiciárias e policiais.

Paralelamente, a necessidade de obtenção de prova digital tornou-se transversal à investigação criminal. Segundo dados da Comissão Europeia amplamente citados no debate legislativo europeu, a prova eletrónica é relevante em cerca de 85% das investigações criminais, e em dois terços desses casos a sua obtenção exige um pedido dirigido a prestadores de serviços sediados noutras jurisdições. Nenhuma investigação criminal minimamente competente – seja de tráfico de estupefacientes, corrupção, abuso sexual de crianças ou terrorismo, mas também em todo o tipo de criminalidade económico-financeira ou com um reflexo patrimonial – pode hoje prescindir de uma abordagem judiciária à recolha, preservação e valoração de prova em formato digital.

É neste contexto que o presente e-book se inscreve e afirma a sua utilidade, resultando do seminário «Cibercrime e *e-evidence*» realizado no Centro de Estudos Judiciários em 20 de abril de 2026, reunindo os contributos dos oradores aí presentes, compreendendo:

– Uma análise dos principais tipos legais da Lei do Cibercrime, com atenção à jurisprudência recente e às alterações introduzidas pelo Decreto-Lei n.º 125/2025, de 4 de dezembro;

– Um olhar prático sobre a aplicação dos artigos 15.º e 17.º da mesma lei, tendo como pano de fundo a mais recente jurisprudência dos Tribunais da Relação, do Supremo Tribunal de Justiça e do Tribunal Constitucional;

– Um estudo sistemático dos instrumentos de cooperação judiciária internacional para a obtenção de prova digital, percorrendo a Lei do Cibercrime, a Convenção de Budapeste e o seu Segundo Protocolo Adicional, o pacote legislativo europeu de *e-evidence* e a recente Convenção das Nações Unidas contra o Cibercrime; e, finalmente,

– Uma análise das questões – ainda e sempre (!) – relevantes em matéria de acesso a metadados na sequência da Lei n.º 18/2024, de 5 de fevereiro.

O momento não poderia ser mais propício.

O Regulamento (UE) 2023/1543 será plenamente aplicável a partir de 18 de agosto de 2026, e a Proposta de Lei n.º 83/XVII/1.ª encontra-se em fase de apreciação parlamentar, visando transpor a Diretiva (UE) 2023/1544 e estabelecer o regime sancionatório interno exigido pelo Regulamento. A entrada em vigor deste novo quadro normativo representará uma mudança de paradigma na forma como as autoridades judiciárias acedem a prova eletrónica detida por prestadores de serviços estabelecidos noutros Estados-Membros, e exigirá preparação por parte das autoridades judiciárias, das autoridades policiais e dos prestadores de serviços digitais.

O CEJ acompanhará de perto as evoluções que se seguirão à plena aplicação deste regime, incorporando na sua oferta formativa as respostas às questões práticas e dogmáticas que a aplicação dos novos instrumentos inevitavelmente suscitará. Este e-book é um primeiro passo nesse sentido.

Antero Taveira

ÍNDICE

CIBERCRIME E *E-EVIDENCE*

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1. BREVE INCURSÃO SOBRE ALGUNS TIPOS LEGAIS EM SEDE DE CIBERCRIME[1]

Rui Teixeira*

Bibliografia
Vídeo da intervenção

*The term "computer piracy" does not exist in portuguese juridical terms. It is a day-to-*day expression that includes all of the computer crimes that exist in the law n.º 109/91 of August 17th.

The law is based on a Counsel of Europe Recommendation and it is an almost exact replica of it.

The courts have not had a chance of making a broad use of it mainly because the issues that are dealt in the law have not become acute. However the known court decisions on these matters reflect the ability of the courts to adapt to new circumstances and to create a all new judicial language and ability to evaluate new situations.

The courts have been helped in this new field by the work that has been done in the universities but have, themselves, began to make their own interpretation of the law, thus clarifying the law n.º 109/91 that has used a technique unlike any other used in the Portuguese legal system save that of the anti-economical crime.

* * *

Quando Philippe Dreyfus propôs, em 1962, o termo *informatique* – contracção das palavras *information* e *automatique* –, depois adoptado pela prestigiada Academia Francesa, estaria longe de suspeitar que o mesmo, poucos anos depois, viria a qualificar uma nova forma de criminalidade e das mais nefastas.

Este tipo de criminalidade acaba assim por revestir um dos novos meios de execução criminosa que, não obstante as vozes que em sentido contrário se levantaram, vai para além do âmbito do crime económico onde conceptualmente acabou por ser inserido.

Consoante a utilização que lhe é dada, o computador pode surgir como:

- objecto do crime (quando a infracção tenha como escopo o próprio equipamento);
- sujeito do crime (quando a infracção tenha uma natureza que poderemos designar por essencialmente informática, ou seja, quando o resultado não pode ser obtido por outros meios);
- instrumento do crime (quando estão em causa delitos ditos clássicos que, teoricamente possam ser cometidos por outros meios e produzir resultados similares, mas em que se optou pelas facilidades proporcionadas pela informática).

[1] Artigo desenvolvido a partir da comunicação apresentada pelo autor no Seminário «Cibercrime e *e-evidence*», realizado em Lisboa, em 20 de abril de 2026, no Centro de Estudos Judiciários.
* Juiz Desembargador em funções no Tribunal da Relação de Lisboa.

Deste modo entendemos que o crime informático tem como âmbito o uso do computador sendo a ilicitude que as condutas acarretam genérica.

Em conclusão: **O crime informático é todo o acto considerado ilícito, cometido por recurso à tecnologia informática, cujas características especificas são intencionalmente procuradas e/ou aproveitadas pelo agente.**

Vejamos agora qual a resposta que o legislador português deu à questão da criminalidade informática sendo que o enfoque será feito a tipos específicos do nosso ordenamento tentando dar a conhecer a forma como os Tribunais portugueses responderam à questão da "pirataria informática".

O termo "pirataria informática" existe na língua portuguesa, mas não se traduz num conceito jurídico. Trata-se de um termo vulgarizado na expressão popular e, empiricamente, se dirá que se refere ao acesso ilegítimo a um conjunto de informação confidencial ou não acessível. Contudo, a legislação portuguesa foi mais longe e criminalizou, desde 1991, de uma forma sistemática outros comportamentos. Serão estes que analisaremos, um a um, deixando apenas de fora aqueles que, pela sua especificidade respeitam a matérias em que o bem jurídico protegido suplanta a forma como o crime é executado.

A criminalidade informática está, grosso modo, prevista na Lei n.º 109/2009, de 15.09 e segue na esteira de uma outra, anterior, a Lei n.º 109/91, de 17.08. que expressamente revogou.

Na elaboração deste diploma legal, transpôs-se para a ordem jurídica a Decisão Quadro 2005/222/JAI, do Conselho, de 24 de Fevereiro, e nela seguiram-se de perto as listas de ilícito que a Recomendação n.º R (89) 9 do Conselho da Europa tinha criado, bem como o relatório e conclusões finais da OCDE sobre esta matéria.

A Decisão Quadro 2005/222/JAI, do Conselho, de 24 de Fevereiro, foi entretanto revogada pela Directiva 2013/40/EU, do Parlamento Europeu e do Conselho, de 12 de Agosto. Esta Directiva 2013/40/EU não foi transposta para o nosso ordenamento apesar do prazo limite para a sua transposição ter ocorrido em 04.09.2015.

Sem prejuízo, a nossa Lei dá já cumprimento a diversos aspectos desta Directiva, designadamente a criminalização de condutas ali previstas.

Contudo, a Lei n.º 109/2009, de 15.09, foi alterada pela Lei n.º 79/2021, de 24 de Novembro, que transpôs a Directiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário.

Já no final do ano passado o Decreto-Lei n.º 125/2025, de 04 de Dezembro, transpôs para a legislação nacional a Directiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União a qual alterou o artigo 4.º, alínea h), que passou a ter a seguinte redacção:

«*'Vulnerabilidade', uma fragilidade, susceptibilidade ou falha, que afecta redes e sistemas de informação, produtos ou serviços de tecnologias da informação ou comunicação, passível de ser explorada por uma ciberameaça, definida na acepção do ponto 8 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de Abril de 2019.*»

Mas mais importante foi o aditar do artigo 8.º A à Lei da Criminalidade informática. Dispõe o novo preceito que:

*"**Artigo 8.º A***
Actos não puníveis por interesse público de cibersegurança

1 - Não são puníveis factos susceptíveis de consubstanciar os crimes de acesso ilegítimo e de intercepção ilegítima previstos, respectivamente, nos artigos 6.º e 7.º, se verificadas, cumulativamente, as seguintes circunstâncias:

a) O agente actue com a intenção única de identificar a existência de vulnerabilidades em sistema de informação, produtos e serviços de tecnologias de informação e comunicação, que não tenham sido criadas por si ou por terceiro de quem dependa, e com propósito de, através da sua divulgação, contribuir para a segurança do ciberespaço;
b) O agente não actue com o propósito de obter vantagem económica ou promessa de vantagem económica decorrente da sua acção, sem prejuízo da remuneração que aquele obtenha como contrapartida da sua actividade profissional;
c) O agente comunique, imediatamente após a sua acção, as eventuais vulnerabilidades identificadas, ao proprietário ou pessoa por ele designada para gerir o sistema de informação, produto ou serviço de tecnologias de informação e comunicação, ao titular de quaisquer dados obtidos e que se encontrem protegidos ao abrigo da legislação aplicável em matéria de protecção de dados pessoais, designadamente, o Regulamento Geral de Protecção de Dados (RGPD), aprovado pelo Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, a Lei n.º 26/2016, de 22 de Agosto, na sua redacção actual, a Lei n.º 58/2019, de 8 de Agosto, e a Lei n.º 59/2019, de 8 de Agosto;
d) A actuação do agente seja proporcional aos seus propósitos e estritamente limitada pelos mesmos, bastando-se com as acções necessárias à identificação das vulnerabilidades e não provocando:

i) Uma perturbação ou interrupção do funcionamento do sistema ou serviço em causa;
ii) A eliminação ou deterioração de dados informáticos ou a sua cópia não autorizada;
iii) Qualquer efeito prejudicial, danoso ou nocivo sobre a pessoa ou entidade afectada, directa ou indirectamente, ou sobre quaisquer terceiros, excluindo os efeitos correspondentes ao próprio acesso ilegítimo ou intercepção ilegítima, nos termos previstos nos artigos 6.º e 7.º, e ainda os que resultariam já, com elevada probabilidade, da própria vulnerabilidade detetada ou da sua exploração;

e) A actuação do agente não consubstancie violação de dados pessoais protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais, designadamente, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, da Lei n.º 58/2019, de 8 de Agosto, e da Lei n.º 59/2019, de 8 de agosto.

2 - A comunicação prevista na alínea c) do número anterior deve ser feita também à autoridade nacional de cibersegurança, que a remete à Polícia Judiciária sempre que revista relevância criminal.

3 - Para efeitos de determinação da proporcionalidade da actuação do agente, tomar-se-á em conta se a mesma era necessária à detecção da vulnerabilidade e se a extensão dos sistemas ou dados informáticos acedidos, consultados e/ou copiados era imposta pelo interesse em contribuir para a segurança do ciberespaço, sendo expressamente vedado o uso das seguintes práticas:

a) Mecanismos de negação de serviço (DoS) ou negação de serviço distribuída (DDoS);
b) Engenharia social, definido como facto de enganar de responsáveis ou utilizadores dos sistemas de informação com vista à disponibilização de informação sensível ou sigilosa;
c) 'Phishing' e variantes;
d) Roubo ou furto de palavras-passe ou outras informações sensíveis;
e) Eliminação ou alteração dolosa de dados informáticos;
f) Inflição dolosa de danos ao sistema de informação;
g) Instalação e distribuição de software malicioso.

4 - Sem prejuízo das regras aplicáveis em matéria de protecção de dados, os dados informáticos que sejam comunicados ao proprietário ou pessoa encarregue da gestão do sistema de informação, produto e serviço de tecnologias de informação e comunicação, ou à autoridade nacional de cibersegurança devem ser eliminados no prazo de 10 dias contados a partir do momento em que a vulnerabilidade for corrigida, devendo garantir-se a sua natureza secreta durante todo o procedimento.

5 - Não são igualmente puníveis os factos praticados com consentimento do proprietário ou administrador de sistema de informação, produto ou serviço de tecnologias de informação e comunicação, sem prejuízo do dever de notificação das vulnerabilidades eventualmente identificadas à autoridade nacional coordenadora encarregada da resposta a incidentes de cibersegurança das vulnerabilidades eventualmente identificadas, nos termos previstos no regime jurídico da cibersegurança.»

A importância e relevância deste preceito e a sua influência sobre o desenho típico da Lei será analisada infra com mais detalhe.

Quanto aos tipos.

O capítulo II da Lei da Criminalidade Informática tem como título "Disposições materiais penais"

No artigo 3.º da dita lei surge o **crime de falsidade informática**.

Dispõe o preceito que:

"1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem é punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

2 - Quando as acções descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para

si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4 - Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

O **interesse protegido pela norma** é a segurança e a fiabilidade de documentos ou outros instrumentos digitais.

Ainda assim o interesse não difere do interesse protegido pelo crime de falsificação existente, apenas se alargando o quadro desses mesmos interesses.

Como **elementos objectivos** deste tipo de crime temos:

- o meio ou actividades realizadas para executar o facto ilícito, ou seja, introduzir, modificar, pagar, suprimir ou, de acordo com a cláusula geral, de por qualquer forma, interferir num tratamento informático de dados. Por outras palavras, a acção consiste em modificar dados já armazenados ou armazenar novos com o mesmo fim ou utilizá-los nas referidas condições, sendo necessário que a visualização desses dados seja equiparável à existência de um documento não autêntico ou falsificado, ou seja, introduzir, modificar, apagar, suprimir ou, por qualquer outra forma – cláusula geral – interferir num tratamento de dados informático; o objecto da acção são esses mesmos dados ou programas informáticos
- o objecto sobre que incide a acção – dados ou programas informáticos;
- a produção de dados ou documentos não genuínos.

Como **elemento subjectivo** temos o dolo nos termos gerais a que acresce um dolo específico que se caracteriza:

a) Pela intenção de que os dados ou documentos não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem;
b) e pelo fim de enganar nas relações jurídicas.

Na anterior redacção só se conferia protecção aos documentos (digitais) que pudessem servir de meio probatório.

Agora o enfoque é outro e é subjectivo.

São protegidos todos os documentos não sendo admissível a sua adulteração sendo que, se a mesma ocorrer, o agente tem de agir com a intenção de que os documentos falsificados sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem.

Em conclusão: o legislador substituiu os elementos do tipo em que fracassavam os tipos tradicionais por outros elementos típicos equivalentes, adaptando-os às notas especificas da criminalidade informática.

Denota-se assim que o texto vem positivar o que face à moderna tecnologia possibilitada pelos computadores já se verificava, ou seja, "*considerados ou utilizados para finalidades juridicamente relevantes como se o fossem*" de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado.

O tipo legal visa equiparar a falsificação de dados à falsificação de documentos no sentido tradicional desde que os dados possam ser considerados ou utilizados para finalidades juridicamente relevantes como se o fossem

O artigo faz referência às mesmas manipulações de dados e programas informáticos que para a fraude informática contendo uma cláusula geral: "*quem, ... por qualquer outra forma, interferir num tratamento informático de dados*".

A disposição em causa aplica-se igualmente aos casos em que os dados manipulados não são transpostos para um texto impresso, mas são directamente empregues para outros tratamentos informáticos, como pode acontecer, p. ex. em transacções bancárias, ou em pagamentos. Enfim, as considerações subjectivas, o elemento intencional, correspondem às que se aplicam à falsificação de documentos *tout court*.

O n.º 2 do preceito mais não é do que a agravação do tipo geral previsto no n.º 1.

Na verdade, aqui apenas se introduz uma especificidade: que as acções descritas no número anterior incidam

a) sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou;
b) serviço de acesso condicionado.

Trata-se de agir, falsificando dados em telemóveis, terminais ATM, POS ou semelhantes, ou sistemas de *homebanking* ou equivalentes.

Aqui a pena é mais grave dado que não admite a opção pela pena de multa mas sim e apenas a pena de prisão com o mínimo de um ano.

No n.º 3 deste artigo prevê-se a responsabilização pelo uso destes documentos quando se actue com intenção de causar prejuízo a outrem ou de obter benefício ilegítimo.

O n.º 3 do preceito é destinado apenas ao que utiliza o documento em questão e não ao falsificador, como aludia o n.º 1.

Trata-se do equivalente informático do crime de uso de documento falsificado previsto e punido pelo artigo 256.º, n.º 1, alínea e), do Código Penal. Nele é necessário o *animus lucrandi* ou

animus nocendi, enquanto o n.º 1 se basta com o requisito objectivo da violação e o subjectivo da consciência do mesmo.

A pena do uso do documento falsificado informaticamente é a mesma que a da falsificação informática, à semelhança do que acontece com a falsificação de documentos tradicional em que a pena as alíneas a) e e) do artigo 256.º, n.º 1, do Código Penal é a mesma, operando-se a diferença em sede de medida concreta da pena nos termos do artigo 72.º do Código Penal.

No n.º 4 já não se pune, propriamente, o acto de falsificar em qualquer uma das suas modalidades, mas sim o produzir, o importar, distribuir, vender ou deter qualquer programa, dados informáticos ou dispositivo que seja passível de permitir o acesso – leia-se o acesso ilícito – a sistemas de comunicações ou acesso condicionado.

Note-se que o crime não pressupõe o resultado da acção. Não é necessário que os dispositivos, programas ou dados sejam efectivamente utilizados. Basta que sejam aptos ao fim o qual mais não é do que adulterar os dados existentes em dispositivos que acedam a sistemas de comunicações ou serviços de acesso condicionado.

No n.º 5 prevê-se uma agravação da pena para o caso da prática dos actos por funcionário em exercício das suas funções.

A tentativa no tipo geral (n.º 1) é punível e o crime é público (ou seja, não depende de apresentação de queixa ou acusação particular bastando-se com a mera denúncia ou conhecimento dos factos por parte do Ministério Público).

Conforme já se disse este tipo traduz-se num alargamento ou ampliação da noção tradicional de documento, tal qual vem definido no Código Penal, de modo tal que se faz uma equiparação da falsificação de dados à falsificação de documentos no sentido clássico do termo, punida no artigo 256.º do Código Penal.

Deste modo para que se verifique a prática deste crime sempre é necessária a produção de uma alteração nos dados ou programas informáticos de modo a que a resposta que o utilizador do sistema, dados ou programa, obtenha não corresponda à verdade.

Não obstante a supressão na actual Lei da referência à susceptibilidade dos documentos servirem como meio de prova, entendemos, contudo, e dado alargamento operado pela alteração da redacção, que têm os mesmos dados ou programas de possuir as características essenciais que se exigem aos documentos probatórios tais como:

a) consubstanciar uma declaração;
b) reconhecer-se, ou ser reconhecível, o seu autor;
c) ter uma função de perpetuação da declaração inserida no documento;
d) ter aptidão para constituir meio de prova no âmbito do tráfico jurídico;

Deste modo as acções levadas a cabo neste tipo acabam por se traduzir na introdução de dados ou programas falsos, na modificação de dados ou programas existentes, em apagar ou suprimir

dados ou programas existentes ou por qualquer outro meio interferir no tratamento informático de dados.

Por último cumpre referir que entre este tipo e o do artigo 256.º do Código Penal, não existe qualquer concurso, dado o objecto específico de protecção deste tipo.

Em termos jurisprudenciais chamamos à colação os seguintes arestos:

Acórdão da Relação de Lisboa de 15.07.2024 (Processo 670/20.3JGLSB.L1-3)
"Uma das formas de execução que preenche plenamente o crime de falsidade informática é o phishing quando a conduta do agente envolva a criação de páginas na Internet imitadas ou copiadas das dos sites oficiais de certas empresas, instituições, organizações ou outra entidades ou pessoas colectivas legítimas como sejam os Bancos, fazendo-o com a finalidade de obter informações sensíveis de natureza bancária, financeira ou outra que seja pessoal ou deva ser considerada confidencial através da indução da vítima em erro."

Acórdão da Relação de Coimbra de 11.10.2023 (Processo 1158/19.0T9CTB.C1)
I – As condutas típicas definidas nas alíneas a), b) e c) do n.º 1 do artigo 256.º do Código Penal inscrevem-se no domínio da «falsificação material», ou seja, corresponde a uma falsificação externa de um documento enquanto objeto que corporiza uma declaração.
II – É no contexto da falsificação material que se inscreve a contrafacção de documento, isto é, o acto de formar um documento até aí não existente por pessoa diversa daquela que aparenta ser o seu autor
III – A alínea d) do n.º 1 do artigo 256.º do Código Penal só cobre a prática das chamadas «falsificações ideológicas», da lavra de quem foi o seu autor, constantes de documentos narrativos, isto é falsificações que tornam o documento inverídico, abrangendo os casos em que o documento incorpora uma declaração escrita, integrada no documento, distinta da declaração prestada, ou seja falsidade intelectual, e os casos em que se presta uma declaração de facto falso juridicamente relevante, ou seja uma narração de facto falso, ou seja, falsidade em documento.
IV – Constituindo a falsidade em documento uma narração de facto falso juridicamente relevante, é consensual que nela não se abrange a simulação, pois o que nesta ocorre é uma declaração de vontade falsa, mas aquilo que consta do documento é exatamente o que as partes declararam.
V – Na revisão de 1995 do Código Penal o legislador eliminou da incriminação da falsificação de documento a falsa documentação indireta, prevista no anterior artigo 233.º, n.º 2, tendo as declarações de factos prestadas a um funcionário para que ele as consigne em documento dotado de fé pública deixado de ter relevo típico.
VI – Não obstante a arguida, para não pagar serviços de telecomunicações, ter indicado à operadora de telecomunicações em conversação telefónica o nome do seu filho menor, que estava à guarda do pai, como titular do contrato de prestação de serviços de fornecimento de internet e de telefone que estava a realizar, nesta conversação ela limitou-se a emitir uma declaração de vontade verbal, sem ter o poder de emitir, elaborar ou determinar a emissão de documento, que não emitiu, elaborou ou cuja emissão determinou, havendo correspondência entre os dados registados e o que foi transmitido e não integrando o caso uma situação em que a declaração seja merecedora de uma credibilidade reforçada, não ocorre o crime de falsificação de documento.
VII – Neste caso verifica-se o crime de falsidade informática, porque os programas instalados no sistema informático trabalharam com dados falsos, uma vez que a verdadeira emitente da declaração foi a arguida, o que gerou um resultado não genuíno dado que quem figurava como contratante não era quem contratou, pondo em causa a integridade dos sistemas de informação.
VIII– Trata-se de um caso de autoria mediata, na medida em que a arguida determinou outrem a praticar os actos de execução necessários à consumação do crime sem nunca perder o domínio do facto.

IX – O bem jurídico tutelado pelo crime de falsidade informática é a integridade dos sistemas de informação, através da qual se pretende impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas de redes e dados.
X – O tipo objectivo do crime preenche-se com a introdução, modificação, apagamento ou supressão de dados informáticos ou por qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, consumando-se o crime apenas com a produção deste resultado.

Acórdão da Relação do Porto de 26.05.2015 (Processo 35/07.2JACBR.P1)
No crime de falsidade informática (Artigo 3.º n.º 1, da Lei do Cibercrime), os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados.
Comete tal crime quem introduzir no sistema informático de um hospital episódios de cirurgias realizadas em regime de ambulatório como se tivessem sido levadas a cabo em regime de internamento, quando tal não correspondia à realidade.
A relação jurídica que com este comportamento se cria não corresponde à verdade, sendo certo que os dados assim vertidos no sistema informático produzem os mesmos efeitos de um documento falsificado, pondo em causa o seu valor probatório e consequentemente a segurança nas relações jurídicas.

Acórdão da Relação de Évora de 19.05.2015 (Processo 238/12.8PBPTG.E1.)
(…)
3. O crime de falsidade informática previsto no artigo 3.º da Lei n.º 109/2009 visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos.
4. A utilização do nome ou de parte do nome de outrem no nome de utilizador e/ou endereço eletrónico, por parte de quem criou conta de correio eletrónico, traduz, no plano objetivo, a produção de dados ou documentos não genuínos, mediante a introdução de dados informáticos, e é idóneo a fazer crer que foi a pessoa a quem respeita o nome ou parte de nome quem efetivamente criou e utilizou a conta de correio eletrónico em causa.

Acórdão da Relação do Porto de 05.11.2025 (Processo 3419/21.0JAPRT.P2)
Atenta a diversidade de bens jurídicos protegidos verifica-se um concurso efetivo entre o crime de burla informática (artigo 221.º, n.º 1, do Código Penal), o crime de falsidade informática (artigo3.º n.º 1 e 2, da Lei n.º 109/2009, de 15/09) e o crime de acesso ilegítimo (artigo 6.º n.º 1 a 3, da cit. Lei n.º 109/2009).

Na ordem da Lei seguem-se os artigos 3.º-A a 3.º G.

Estes preceitos foram introduzidos pela Lei n.º 79/2021, de 24 de Novembro, e destinaram-se a trazer para a Lei do Cibercrime/Lei da Criminalidade Informática a punição do uso de cartões de crédito que até ali era punida no âmbito do Código Penal.

Os preceitos agora aditados referem-se, pois, quer a cartões de crédito, quer a cartões de débito.

Os preceitos em si são relativamente simples não oferecendo grandes dificuldades dogmáticas.

Dispõe o **artigo 3.º-A**, sob a epígrafe **"Contrafacção de cartões ou outros dispositivos de pagamento"** que:

> "*Quem, com intenção de provocar engano nas relações jurídicas, contrafizer cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, nomeadamente introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos, é punido com pena de prisão de 3 a 12 anos.*"

Convém, desde logo, reter que o preceito se refere, quer a cartões de crédito, quer a cartões de débito ou dispositivos para esse efeito (v.g. *smartwatches* com ligação digital ao banco). Refere-se, outrossim, quer a cartões físicos, quer a cartões virtuais (ou seja, aqueles que existem em ambiente digital e que representam apenas uma forma de acesso digital a fundos, quer a crédito, quer a débito.

São **elementos objectivos** do tipo:

> – Contrafazer cartão de pagamento ou qualquer outro dispositivo – corpóreo ou incorpóreo, que permita acesso a meio ou sistema de pagamento.

De notar que o preceito exige uma modalidade de acção a qual seja que a contrafacção tem de ser feita introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos.

Note-se que a contrafacção que se pune é a contrafacção do cartão ou dispositivo e não a contrafacção do sistema informático.

Assim, se alguém falsifica dados num sistema de um banco e o cartão ou dispositivo permanece intocado agindo apenas em obediência a dados adulterados a montante, o crime em causa não é este, mas sim, em princípio, o do artigo 3.º, n.º 1.

A diferença na pena justifica-se porque neste preceito 3.º-A se está a agir sobre o meio de pagamento com a certeza de um dano proveniente da acção o que não se pressupõe nos casos do artigo 3.º, n.º 1.

E tanto é assim que se exige que a contrafacção interfira no tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos.

Subjectivamente exige-se:

- dolo genérico;
- dolo específico: provocar engano nas relações jurídicas.

O artigo 3.º B com a epígrafe "**Uso de cartões ou outros dispositivos de pagamento contrafeitos"** dispõe:

> *1 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.*
>
> *2 - As acções descritas no número anterior são punidas com pena de prisão de 2 a 8 anos se o prejuízo ou o benefício for de valor consideravelmente elevado.*
>
> *3 - As acções descritas no n.º 1 são punidas com pena de prisão de 3 a 12 anos se o agente as praticar de concerto com o agente dos factos descritos no artigo 3.º-A.*

O preceito pune a utilização consciente de cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito.

Trata-se no fundo de dar o passo seguinte à conduta prevista no artigo 3.º A. Neste punia-se a contrafacção. Aqui pune-se o uso do cartão ou dispositivo contrafeito.

Previne-se, claro está, que o uso seja feito por pessoa diferente do falsificador. Se for este a usar o cartão ou dispositivo falsificado a punição é feita pelo artigo 3.º-A.

Contudo, o n.º 3 prevê uma agravação que consiste em existir uma acção concertada com o falsificador. Alei não é clara neste particular usando o termo "concerto". Na verdade, e tendo presente que não se está perante uma co-autoria, vislumbramos estarem aqui abarcadas aquelas situações em que o utilizador está em conluio com o falsificador e em que ambos beneficiam com o uso que o utilizador dá ao cartão ou dispositivo contrafeito.

Só assim se justifica a pena acrescida.

O **artigo 3.º C,** sob a epígrafe "**Aquisição de cartões ou outros dispositivos de pagamento contrafeitos**", dispõe que:

> *"Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos."*

Como a epígrafe sugere pune-se a conduta de quem, tendo na sua disposição, consabidamente, cartão de pagamento contrafeito ou dispositivo que permita o acesso a sistema ou meio de pagamento contrafeito, o transmite a terceiros.

O preceito pretende punir toda o tipo de transmissão como resulta do segmento "*por qualquer forma transmitir ou disponibilizar*".

Pune-se também a aquisição do cartão ou dispositivo assim se completando a punição desde a criação (contrafacção) até ao seu uso final.

Quer o artigo 3.º A, quer o 3.º B, quer o 3.º C, subjectivamente, exigem sempre, a par do dolo genérico, um dolo específico consistente na:

- intenção de causar prejuízo a outrem ou;
- obter benefício ilegítimo.

Esta intenção de causar prejuízo não necessita de ser directa no sentido que o agente sabe ou quer que a vítima "A" ou "B" seja prejudicada.

A Lei basta-se com o conhecimento genérico que a conduta assumida é, dentro da normalidade, apta a causar prejuízo.

Seja como for o dolo específico dos preceitos é alternativo sendo que a Lei se basta com o agente agir com a intenção de obter um benefício ilegítimo.

O **artigo 3.º D** sob a epígrafe "**Actos preparatórios da contrafacção**" dispõe que:

> *"Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer cartão, dispositivo, programa ou outros dados informáticos, ou quaisquer outros instrumentos, informáticos ou não, destinados à prática das acções descritas no artigo 3.º-A, é punido com pena de prisão de 1 a 5 anos."*

O preceito não gera grandes dúvidas quanto à sua interpretação.

Assim, o que se pune é a detenção, aquisição, importação, venda e/ou distribuição de qualquer cartão, programa, dispositivo ou dado informático destinado à prática da contrafacção de cartões ou dispositivos de acesso a sistema ou meio de pagamento contrafeito.

O **artigo 3.º E** sob a epígrafe "**Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático**" dispõe que:

> *"Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar:*
>
> *a) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;*
> *b) Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que haja sido obtido mediante facto ilícito típico previsto*

nos artigos 4.º, 5.º, 6.º e 7.º;

é punido com pena de prisão de 1 a 5 anos."

Aqui a situação já é diferente.

Aqui os dados registados ou os cartões de pagamento ou outros dispositivos são verdadeiros. Nada nos mesmos foram, em si corrompidos.

O que aconteceu foi que os dados, cartões ou dispositivos, foram, em si, obtidos através da prática de crime informático.

São **elementos objectivos** do tipo:

- A aquisição detenção, exportação, importação transporte, distribuição ou venda ou qualquer outra forma de transmissão ou disponibilização de:
- Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento ou;
- Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento

que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

Ou seja, os dados ou cartões de pagamento têm de ser adquiridos através da comissão de crimes de:

- dano informático;
- sabotagem informática;
- acesso ilegítimo; ou
- intercepção ilegítima.

A aquisição de cartões, dados ou dispositivos por outra forma que não a comissão destes crimes informáticos não preenche o tipo, sem prejuízo do preenchimento de outros tipos legais.

São **elementos subjectivos** do tipo:

- dolo genérico;
- dolo específico: actuar com a intenção de causar prejuízo a outrem ou obter benefício ilegítimo.

O artigo 3.º F dispõe, sob a epígrafe de "**agravação**" que:

"Se os factos referidos nos artigos 3.º-A a 3.º-E forem praticados por funcionário no exercício das suas funções, o limite mínimo da pena de prisão aplicável é:

a) De 2 anos, tratando-se dos factos previstos no n.º 1 do artigo 3.º-B, no n.º 1 do artigo 3.º-C, no artigo 3.º-D e no artigo 3.º-E;
b) Agravado em um terço, nos restantes casos."

O preceito nada de especial tem remetendo-se para o artigo 386.º do Código Penal.

O **artigo 3.ºG**, por sua vez, dispõe:

"Para efeitos da presente lei, considera-se também sistema ou meio de pagamento aquele que tenha por objecto moeda virtual."

Trata-se de alargar o âmbito da Lei da moeda com curso legal para a moeda virtual.

O artigo 4.º da Lei da Criminalidade Informática refere-se ao **crime de dano relativo a dados ou programas informáticos.**

Dispõe o preceito que:

"1- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

2 - A tentativa é punível.

3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.

4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa."

O bem jurídico protegido pela norma é a integridade e o bom funcionamento ou o bem uso de dados e programas informáticos.

A especialidade dos danos reside no facto de que não se trata de lesar a substância de um objecto e, por isso, entravar a sua utilização, mas sobretudo de modificar a qualidade das informações contidas nos dados ou programas registados, o que, de toda a evidência, pode diminuir o seu potencial – normalmente ocorre através da introdução de vírus, bombas lógicas ou informáticas, *screen savers* irrecuperáveis, *passwords* e ficheiros biodegradáveis. Contudo, e é isto que caracteriza a figura, é que o alvo são os programas e não sistema informático.

Assim como **elementos objectivos** do tipo temos:

a) falta de autorização;
b) a actividade típica – apagar, alterar, destruir – no todo ou em parte –, danificar, suprimir, tornar não utilizável ou acessível ou de qualquer forma afectar a capacidade de uso dos dados ou programas informáticos;
c) objecto da actuação típica: dados ou programas informáticos alheios.

Como **elemento subjectivo** do tipo temos a exigência do dolo nos termos gerais.

Prevê-se no n.º 2 a punibilidade da tentativa, sendo certo que para que esta possa existir é necessário que o agente já tenha acedido aos dados ou programas informáticos, com intenção de os destruir, mas que ainda não tenha conseguido proceder a tal intento.

No entanto, cumpre referir que se trata de uma situação de difícil detecção a que acresce que esta mesma tentativa acaba por configurar o tipo do artigo 6.º – acesso ilegítimo – mas sempre se punirá pela tentativa de dano deste artigo, atenta a moldura penal mais gravosa.

O n.º 3 pune a produção, venda e distribuição, por qualquer forma, bem como a introdução num ou vários sistemas de programas ou outros dados informáticos destinados a produzir o dano punido pelo n.º 1.

Trata-se no fundo de punir a introdução de vírus e outras aplicações cuja função é causar danos num sistema.

Prevêem-se agravações da pena em função do valor económico dos danos nos n.ºs 4 e 5.[2]

No n.º 6 faz-se depender de queixa o procedimento para os crimes previstos no n.º 1, 2 e 4.

Já o crime previsto no n.º 4 é de natureza pública.

Como salienta Pedro Miguel Januário Lourenço[3] "é imperioso notar que actualmente o facto de haver um dano informático num banco, num hospital, numa instituição pública, entre outros, poderá representar riscos muito grandes para a sociedade, inclusivé para a própria vida humana, pelo que o legislador quis incutir aqui um desejo de paz social que não pretende ver fragilizado pelo recurso aos sistemas de informação".

O artigo 5.º da Lei da Criminalidade Informática refere-se ao crime de **sabotagem informática.**

Dispõe o preceito que:

[2] Cfr. artigo 202.º do Código Penal.
[3] In Estudos do Direito da Comunicação, Instituto Jurídico da Comunicação, Faculdade de Direito de Coimbra, Coimbra 2002, pág. 336.

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - Nos casos previstos no número anterior, a tentativa não é punível.

4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5 - A pena é de prisão de 1 a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;
b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos."

O bem jurídico protegido pela norma é o interesse do proprietário ou do utente de um sistema informático ou de um sistema de telecomunicações em que eles estejam em condições correctas de funcionamento.

Até aqui, há evidentes semelhanças com o tipo de crime anterior, no tocante ao dano em referência ao bem jurídico objecto de protecção.

É assim um crime de dano ou resultado dado que se exigem as alterações mencionadas no tipo. O elemento específico deste crime reside na intenção de entravar o funcionamento dos referidos sistemas.

São elementos constitutivos do tipo qualquer tipo de ingerência num sistema informático, sendo que os meios específicos são exemplos padrão, e que o objectivo do autor do crime se consubstancia na intenção de encravar o funcionamento do sistema informático ou de telecomunicações.

Assim como **elementos objectivos** do tipo temos:

- a actividade típica de introduzir, alterar, deteriorar, danificar, apagar ou suprimir dados ou programas informáticos, ou por qualquer outra forma neles intervir.

Como **objecto da actuação** temos:

- o sistema informático ou sistema de telecomunicações de dados à distância.

Como **elemento subjectivo** temos:

- o dolo nos termos gerais a que acresce um elemento subjectivo específico traduzido na intenção de entravar ou perturbar o funcionamento do sistema de comunicações.

No n.º 2 pune-se a produção, venda e distribuição, por qualquer forma, bem como a introdução num ou vários sistemas informáticos de dispositivos, programas ou outros dados informáticos destinados a produzir a sabotagem punida pelo n.º 1.

Trata-se no fundo de punir a introdução de vírus e outras aplicações cuja função é causar a paralisia ou desvirtuamento de um sistema.

No n.º 3 declara-se que a tentativa, nos casos do n.º 2, não é punível. A razão é simples: a introdução (ou tentativa de introdução) de um vírus ou programa que não alcança o seu fim redunda numa tentativa impossível, logo não punível.

Nos n.ºs 4 e 5, alínea a), prevê-se uma agravação da pena em função do valor económico da perturbação.

No n.º 5, alínea b), a agravação é em função do alvo da sabotagem desde que perturbação seja de forma grave e duradoura.

A forma de actuar em caso de sabotagem é ou pode ser semelhante no preenchimento do tipo do artigo 4.º e no tipo do artigo 5.º.

De facto, estes preceitos são o terreno de eleição dos vírus, dos *worms*, dos *trojans* ou das bombas-relógio, sendo, quanto a nós, o artigo 5.º o local onde o SPAM[4] (pelo menos algum SPAM) é criminalmente punido.

Os vírus são programas, auto executáveis nos computadores para onde são enviados, que se alocam a todo o tipo de suportes em que são utilizados e que produzem ordem desde o simples comando "del*.*" até outros que possam porventura, apenas "brincar" com o utilizador.

Normalmente o vírus apresenta três elementos caracterizadores: a capacidade de se duplicar, a de activar-se sem intervenção humana e a de eliminar o conteúdo do nosso sistema. Podem ainda funcionar como bombas-relógio, ou seja activarem-se numa dada hora ou dia pré-programada.

Worms são uma espécie de vírus[5] que provocam efeitos ainda mais nocivos, porque além do comando principal e das demais características, propagam-se pelas redes onde são instalados, levando consigo em alguns casos informação confidencial do sistema onde são alojados, porventura violando segredos.

---

[4] A palavra SPAM é originária de uma série de comédia de *Monthy Python* onde *vikings* desajeitados pediam, num bar, incessantemente SPAM, marca de um presunto enlatado norte americano.

[5] Por exemplo, o Code Red II que atacou o Pentágono, a Casa Branca e até a Assembleia da República Portuguesa (ver *Computerworld* de 18 a 24 de Outubro, ano 15, n.º 474).

Trojans consistem em vírus que surgem sob a forma de um ficheiro de oferta e que, uma vez aceite e uma vez no interior do computador, destroem ou efectuam comandos.

Por fim, *o SPAM* ... o *SPAM* é basicamente o envio de correio electrónico não solicitado por norma em quantidade superior a um e sem interesse para o destinatário.

Quanto ao expedidor ele representa lucros significativos sendo que nalguns casos representa um custo inferior em 50 vezes ao envio de uma carta de correio em serviço de mailing tradicional.

O *SPAM* tem, *regra geral,* as seguintes características:

1. não é solicitado pelo receptor;
2. a identificação do remetente é falsa;
3. é usada a máquina servidora de correio electrónico de uma vítima, seja de um ISP ou de uma entidade pública ou privada.

Em Portugal é este terceiro ponto que confere a tipificação criminosa a quem envia o "spam", uma vez que, quem naqueles termos usar um servidor de e-mail de terceiro pode ser acusado da prática do crime de acesso ilegítimo.

Pode ainda coexistir o crime de falsificação se a identificação de endereço falsificada referida no ponto "2." for a de alguém em concreto.

Se o intuito do "*spam*" é interferir no normal funcionamento de um sistema informático poderá ser considerado crime de sabotagem informática.

No entanto, não nos parece que seja sempre ou necessariamente assim. No entanto, a mesma ainda não pode ser comprovada já que nos tribunais portugueses a questão ainda não se colocou.

Voltando ao *SPAM* ... que acontece quando o *SPAM* que recebemos não obedece, cumulativamente, às três características?

Em Portugal os ISP´s privados não se opõem e não consideram abuso a utilização dos seus servidores de SMTP para o envio de *e-mail*, antes o contratualizam.

Além do mais para existir falsificação ter-se-ia de equiparar um *e-mail* ao envio de uma carta, o que não ocorre senão na situação particular do envio de uma carta com assinatura digital. O direito ao nome não é extensível ao e-mail pelo que este não goza de protecção jurídica e o legislador português não quis punir os “spammers”.

Autores existem, contudo, que defendem que o envio de “SPAM” é sempre criminalmente punido.

Efectivamente, o envio de *SPAM*, porque visa a interferência em sistema informático, actuando com intenção de o entravar ou de perturbar o seu funcionamento, configura sabotagem informática.

O "spammer" não deseja apenas 'informar' sobre um determinado evento; ele pretende perturbar o próprio sistema informático e por isso envia um elevado número de mensagens diferentes ou um elevado número de mensagens diferentes[6] já que o princípio do "spamming" é *"Eu quero, eu mando e não pago. Não quer mas terá de receber e pagar".*

Esta posição é refutada, no entanto, por *Pedro Miguel Januário Lourenço*[7] que salienta que o envio de mensagens publicitárias está contemplado no direito de expressão de liberdade publicitária que tem cobertura implícita no artigo 37.º, n.º 1, da Constituição já que existe liberdade de mercado e iniciativa privada que não sobrevive sem a comunicação ao público. Refere o autor que os *spammers* violam em regra o regime de "*opt-in*"[8] e não de "*opt-out*"[9] e se é certo que o "spam" é incomodativo já que nos obriga a perder tempo a apagar correio não menos certo é que ele serve um fim comercial.

No entanto, e quanto a nós existe uma situação em que o *spamming* é criminalmente punido. Trata-se do caso das "mail bombs" em que o objectivo primeiro é o de entupir as caixas de correio ou os servidores, entravando assim o seu funcionamento. Nestes casos e só nestes casos será a conduta punível.

Interessante será a verificação de uma situação de concurso entre os crimes de dano informático e sabotagem informática.

Quanto a nós o bem protegido pelo artigo 6.º, era a segurança do sistema informático, tratando-se de um crime de perigo, ou seja, onde não está presente a necessidade de um resultado típico bastando-se a lei, numa antecipação da tutela penal, com o perigo que a conduta gera e que o artigo 7.º protege o interesse do proprietário em que o sistema funcione, tratando-se de um crime de dano, ou seja, um crime onde se pressupõe um resultado. Assim, o crime do artigo 5.º consome o do artigo 6.º já que existindo um resultado não há que punir o perigo que este já pressupunha.

Embora, como referem *Garcia Marques* e *Lourenço Martins*[10] haja que ter algum cuidado na distinção entre os "prejuízos" (que podem ser materiais ou não) e os danos (que têm de ser necessariamente materiais), a conclusão parece-nos ser esta *desde que o âmbito do perigo seja*

---

[6] Joel Timóteo Ramos Pereira, Direito da Internet e Comércio Electrónico, Quid Juris? – Sociedade Editora, Lisboa, 2001, pág. 250 e 251.
[7] Ob. Cit. pág. 302 a 305.
[8] Abreviatura de *option-in*, ou seja, opção de entrada. Neste regime o visado apenas se vincula à utilização dos seus dados pessoais a partir do momento em que declara expressamente essa intenção.
[9] Abreviatura de *option-out*, ou seja, opção de saída. Neste regime o visado com a utilização dos seus dados pessoais está desde logo vinculado à propaganda em causa, podendo sair desta a todo o momento, através de declaração ao utilizador desses dados a partir do momento em que declara expressamente essa intenção.
[10] In Direito da Informática, Instituto Jurídico da Comunicação, Livraria Almedina, Coimbra, 2000, pág. 527 e 528.

na totalidade abarcado pelo dano. Assim, se com a sua conduta o agente criou um dano mas criou ainda um perigo maior que extravasa o âmbito do dano haverá uma situação de concurso real.

O artigo 6.º da Lei da Criminalidade Informática refere-se ao **crime de acesso ilegítimo.**

Dispõe o preceito que:

"1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - A pena é de prisão até 2 anos ou multa até 240 dias se as acções descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

4 - A pena é de prisão até 3 anos ou multa se:

a) O acesso for conseguido através de violação de regras de segurança; ou
b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

5 - A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

6 - A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.

7 - Nos casos previstos nos n.os 1, 4 e 6 o procedimento penal depende de queixa.

O bem jurídico protegido pela norma é segurança do sistema informático ou aquilo a que se tem chamado a inviolabilidade do domicílio informático.

A infracção tem por fim impedir qualquer penetração nos sistemas ou redes informáticas, ou seja, equivale a uma protecção antecipada e indirecta contra riscos de danos e até da espionagem informática de que se ocupa o artigo 8.º.

Em resumo, o tipo incriminador tem por finalidade reprimir qualquer penetração abusiva em sistemas ou redes informáticas, com o fim de o agente para si ou para terceiro alcançar um benefício ou vantagem ilegítimos.

É o chamado *furtum usus* dado que o agente beneficia pelo facto de estar dentro do sistema ou rede informática, uma vez que a vantagem pode consistir tão só na própria utilização do sistema informático, havendo quem considere isto uma forma especial de furto de serviços.

Como **elementos objectivos** temos assim:

- não ter permissão legal ou não estar autorizado pelo proprietário ou titular do direito do sistema ou parte dele
- aceder, de qualquer modo, a um sistema ou rede informáticos.

Assim, é um crime de execução não vinculada, dado que o agente pode aceder ao sistema ou rede informáticos mediante qualquer forma, ou seja, e a título de exemplo, mediante ou não o uso de password

Como **elemento subjectivo** temos o dolo nos termos gerais não existindo a necessidade de existência de intenção de alcançar para si ou para terceiro benefícios ou vantagem ilegítimas, algo que sucedia antes da entrada em vigor da Lei 79/2021, de 24 de Novembro.

O tipo base é o do n.º 1.

Os demais constituem variações da conduta, senão vejamos.

O n.º 2 pune com a mesma pena do n.º 1 a produção, venda, distribuição ou por qualquer outra forma a disseminação ou introdução num ou mais sistemas informáticos dispositivos, programas, de um conjunto executável de instruções, de um código ou de outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

Trata-se aqui de punir já não quem acede, mas quem fornece os meios ao agente para aceder a sistemas que lhe estão vedados

No n.º 3 prevê-se a agravação da pena em função do objectivo da acção: "acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento"

No n.º 4, alínea b) e 5, alínea a) agrava-se a pena em função do tipo de segredo que se viola com acesso enquanto no n.º 4 alínea a) se agrava a pena em função do tipo de acção, mais concretamente, se o acesso for feito com violação das regras de segurança.

No n.º 5, alínea b), a agravação é feita em função do benefício ou vantagem patrimonial.

Como o tipo de objectivo da acção estão separados caso as circunstâncias coexistam, o preenchimento faz-se em função de cada uma das alíneas reflectindo na medida da pena tais circunstâncias.

O n.º 6 esclarece que a tentativa é punível, excepto nos casos dos n.ºs 2 e 3.

No n.º 7 determina-se que nos casos dos n.ºs 1, 4 e 6 o procedimento criminal depende de queixa.

Neste tipo incluem-se condutas como o "hacking", o "cracking"[11] ou o "phreaking"[12].

De notar que muitas vezes o "hacking" é apenas uma forma do agente testar as suas capacidades, uma espécie de teste à "virilidade virtual" do agente (condicente com o perfil típico do autor destes crimes) pelo que, inexistindo qualquer benefício ou vantagem ilegítima, não há crime.

Note-se que a legislação portuguesa, desde a entrada em vigor da Lei n.º 79/2021, de 24 de Novembro, passou a incorporar aquilo que os ingleses chamaram de "pure hacking offense".

Qualquer acesso não consentido, mesmo que dele não resultem quaisquer danos para além do próprio acesso, é punido.

Regressando ao Acórdão da Relação de Lisboa de 15.07.2024, Processo 670/20.3JGLSB.L1-3, aí podemos ler:

> *"(…) não há dúvida de que a entrada num serviço de homebanking prestado pela instituição bancária na qual se encontra domiciliada uma determinada conta bancária usando as credenciais de acesso a essa conta de que um terceiro é titular, sem autorização ou consentimento expresso ou presumido do mesmo configura um acesso ilegítimo relevante para integrar o tipo previsto no artigo 6.º da Lei 109/2009 de 15 de Setembro.*
>
> *Não existe concurso aparente entre o crime de acesso ilegítimo e o crime de burla.*

---

[11] Termo geralmente empregue para se fazer referência à intrusão em sistemas informáticos. As actividades de *hacking* ou de *cracking*, (acesso ilegítimo com intuito de destruição de dados), são, à face da Lei portuguesa, crime de acesso ilegítimo, e por isso punido com pena de prisão até um ano, agravado até três anos ou multa se o acesso for conseguido através de violação de regras de segurança. Cabem nestas punições a utilização sem autorização prévia de *default accounts* e de passwords que lhes não pertençam, como por exemplo, usar as contas de acesso de terceiros para aceder à INTERNET.

[12] Para se compreender o significado é necessário compreender primeiro que existem condutas denominadas *Blackboxing* e *Blueboxing* que contemplam todas as formas de perturbação de telecomunicações, quer por injecção de frequências nas linhas telefónicas quer por ligar a estas dispositivos electrónicos cujo efeito, de entre outros, sejam o impedimento total ou a diminuição da taxação devida à operadora de telecomunicações. *Blueboxing*, que consiste na utilização simultânea de computadores pessoais com possibilidade de processamento de som e de um programa específico, para injectar tons com determinadas frequências nas linhas telefónicas, conseguindo forçar centrais telefónicas a deixar de taxar as comunicações efectuadas. Portanto quem faz a chamada não paga.
Inversamente, *Blackboxing* é a designação dada a um conjunto de componentes electrónicos que interligados segundo determinado esquema e desde que ligado à rede telefónica de determinada pessoa, lhe permite receber chamadas evitando a correspondente taxação a quem lhe ligou.
Tais condutas constituem crime de burla nas comunicações, punido pelo artigo 221 n.º 2 do Código Penal com pena até 3 anos de prisão.
No que respeita ao *phreaking*, para além de se aplicarem os mesmos princípios relativos às actividades de *blueboxing*, a utilização de redes de comunicações com base na manipulação de centrais telefónicas acedidas sem autorização para o efeito, constitui o crime de acesso ilegítimo (ver ainda www.ciberjus.org/revista/criminalidade-informatica.html)

No crime de acesso ilegítimo o bem jurídico protegido é a segurança dos sistemas informáticos. A burla, seja ela a informática ou a clássica, visa proteger o património. Pese embora a burla possa estar numa relação de instrumentalidade com o acesso ilegítimo, quando cometida através de meios enganosos que requerem a utilização de dados e sistemas informáticos e que, por isso, mesmo incluí, no seu processo executivo a prática de actos subsumíveis ao crime de acesso ilegítimo, não esgota a ilicitude e a censurabilidade da intrusão e devassa não autorizadas das informações pessoais, de natureza confidencial de outrem, nem neutraliza a diversidade e autonomia dos diferentes bens jurídicos, reclamando, por isso, sanções autónomas."

O artigo 7.º da Lei da Criminalidade informática refere-se ao **crime de intercepção ilegítima**.

Dispõe o preceito que:

1. "*Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.*

2. A tentativa é punível

3. Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número."

É aquilo a que vulgarmente se chama espionagem informática.

Ao lado das pesquisas não autorizadas de dados, é hoje possível colocar sob escuta e vigiar os sistemas de transmissão de dados à distância, bem como interceptar dados em curso de transmissão ou a partir de emissões electrónicas.

O interesse jurídico protegido é para além do direito à vida privada não perturbada, o direito à exclusividade das comunicações de dados à distância.

Conforme o modo de intercepção, a segurança do sistema informático e de telecomunicações pode entrar em crise.

Visa-se, assim, reprimir comportamentos tais como uma colocação sob escuta de sistemas de transmissão de dados à distância, assim como a intercepção de dados em curso de transmissão ou a partir de emissões electrónicas.

Os **elementos objectivos** do tipo são:

- não ter autorização legal ou não estar autorizado
- através de meios técnicos interceptar comunicações que se processam no interior de um sistema ou rede informática, a ele destinados ou deles provenientes.

Como **elemento subjectivo** temos o dolo nos termos gerais.

Entendemos que este tipo se traduz num crime de execução vinculada pois só pode ser cometido através de meios técnicos, os quais podem ser escutas telefónicas, o uso de satélites ou a criação de contas "clone" com "by passes" no servidor por ex.:, para além de que só com a utilização deles é que o agente consegue aceder ao seu objectivo.

A tentativa é punível nos termos do n.º 2.

O n.º 3 antecipa a punição pois pune quem fornece os meios capazes de levar à intercepção ilegítima, sejam eles mecânicos (hardware), sejam informáticos (*software*).

Cumpre referir que, mediante autorização judicial é admissível, a comissão dos factos tipicamente previstos. Na verdade, da mesma forma que é possível a escuta de uma conversação telefónica é possível ao juiz ordenar a intercepção de uma ou várias comunicações "on-line".

Tal autorização está especialmente prevista no artigo 34.º, n.º 4, *in fine* da Constituição da República Portuguesa que prevê expressamente a possibilidade de intercepção na correspondência e telecomunicações sendo que a NET mais não é do que a telecomunicação de dados.

A Constituição vai até mais longe ao referir que é permitida a intercepção dos "demais meios de comunicação".

Existe um concurso aparente entre o n.º 1 e o n.º 3 deste preceito na medida em que ao produzir, vender, distribuir ou, por qualquer outra forma disseminar ou distribuir dispositivos ou dados informáticos nocivos (que precedem necessariamente a ocorrência do acesso ao conteúdo da comunicação) o crime de intercepção ilegítima já está consumado, funcionando a consecução do acesso ao conteúdo da comunicação como agravante da medida da pena nos termos do artigo 71.º, n.º 2, do Código Penal.

O último dos crimes previstos na Lei da Criminalidade Informática, consta **do artigo 8.º** da mesma e é denominado **reprodução ilegítima de programa protegido**.

Dispõe o preceito que:

> *1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.*
>
> *2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.*
>
> *3 - A tentativa é punível.*

É um artigo que gerou muita confusão e controvérsia até à entrada em vigor do D.L. n.º 259/94.

É do conhecimento geral que os programas informáticos constituem um dos principais alvos da criminalidade informática. Pressupõem um enorme investimento de mão de obra em competência científica e técnica, em experiência e tempo.

Deste modo este tipo não mais visa do que proteger o interesse jurídico da propriedade intelectual.

Garante-se ao autor do programa ou ao titular dos direitos, que não terão de lamentar os investimentos consagrados à sua criação.

Este tipo utiliza uma técnica legislativa *sui generis* a que a doutrina usa chamar de técnica de reenvio, dado que refere "programa informático protegido por lei", estando naturalmente a reenviar para outra legislação, inclusivamente extra-penal, que deve dizer que programas são protegidos e em que condições.

Trata-se de um crime material ou de dano.

Como **elementos objectivos** do tipo temos:

- a falta de causa legítima para a acção;
- a acção que consiste em reproduzir, divulgar ou comunicar ao público;
- o objecto da acção é o programa informático protegido por lei.

Como **elemento subjectivo** temos o dolo nos termos gerais.

A conduta punida pode assumir três modalidades distintas:

a) a reprodução (tendo-se em atenção, no entanto, o fim da mesma já que a reprodução por um utente legítimo para fins de back-up, teste, estudo ou ensaio, é legalmente admissível)[13]
b) divulgação ao público;
c) comunicação ao público.

Especial relevância nesta temática assume a questão do concurso de normas, especialmente entre si e com uma outra: a burla informática.

Salientou-se no Acórdão do Supremo Tribunal de Justiça de 05.11.2008, Processo 08P2817, que: *"A problemática relativa ao concurso de crimes (unidade e pluralidade de infracções), das mais complexas na teoria geral do direito penal, tem no artigo 30.º do Código Penal a indicação de um princípio geral de solução: o número de crimes determina-se pelo número de tipos de crime efectivamente cometidos, ou pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente.*

[13] Vide artigo 6.º do D.L. n.º 252/94.

O critério determinante do concurso é, assim, no plano da indicação legislativa, o que resulta da consideração dos tipos legais violados. E efectivamente violados, o que aponta decisivamente para a consagração de um critério teleológico referido ao bem jurídico.

A indicação da lei acolhe, pois, as construções teoréticas e as categorias dogmáticas que, sucessivamente elaboradas, se acolhem nas noções de concurso real e concurso ideal.

Há concurso real quando o agente pratica vários actos que preenchem autonomamente vários crimes ou várias vezes o mesmo crime (pluralidade de acções), e concurso ideal quando através de uma mesma acção se violam várias normas penais ou a mesma norma repetidas vezes (unidade de acção).

O critério teleológico que a lei acolhe no tratamento do concurso de crimes, condensado na referência a crimes «efectivamente cometidos», é adequado a delimitar os casos de concurso efectivo (pluralidade de crimes através de uma mesma acção ou de várias acções) das situações em que, não obstante a pluralidade de tipos de crime eventualmente preenchidos, não existe efectivo concurso de crimes (os casos de concurso aparente e de crime continuado).

Ao lado das espécies de concurso próprio (ideal ou real) há, com efeito, casos em que as leis penais concorrem só na aparência, excluindo uma as outras. A ideia fundamental comum a este grupo de situações é a de que o conteúdo do injusto de uma acção pode determinar-se exaustivamente apenas por uma das leis penais que podem entrar em consideração - concurso impróprio, aparente ou unidade de lei.

A determinação dos casos de concurso aparente faz-se, de acordo com as definições maioritárias, segunda regras de especialidade, subsidiariedade ou consunção.

Especialmente difícil na sua caracterização é a consunção. Diz-se que há consunção quando o conteúdo de injusto de uma acção típica abrange, incluindo-o, outro tipo de modo que, de um ponto de vista jurídico, expressa de forma exaustiva o desvalor (cfr. v. g. H. H. JESCHECK e THOMAS WEIGEND, "Tratado de Derecho Penal", 5.ª edição, p. 788 e seguintes.).

A razão teleológica para determinar as normas efectivamente violadas ou os crimes efectivamente cometidos, só pode, pois, encontrar-se na referência a bens jurídicos que sejam efectivamente violados. O critério do bem jurídico como referente da natureza efectiva da violação plural é, pois, essencial.

O critério operativo de distinção entre categorias, que permite determinar se em casos de pluralidade de acções ou pluralidade de tipos realizados existe, efectivamente, unidade ou pluralidade de crimes, id. est, concurso legal ou aparente ou real ou ideal, reverte ao bem jurídico e à concreta definição que esteja subjacente relativamente a cada tipo de crime.

Ao critério de bem jurídico têm de ser referidas as soluções a encontrar no plano da teoria geral do crime, sendo a matriz de toda a elaboração dogmática (cfr. acórdão do Supremo Tribunal de Processo n.º 1942/06-3ª).”

Por sua vez, no Acórdão do Supremo Tribunal de Justiça de 12.07.2012, Processo 1718/02.9JDLSB, considerou-se:

"I - O tipo legal é o portador, o interposto da valoração jurídico-criminal, ante o qual se acham colocados os tribunais e o intérprete. A possibilidade de subsunção duma relação da vida a um ou vários tipos legais de delito é a chave para determinar a unidade ou pluralidade a unidade ou pluralidade de crimes.

II - A consideração da «culpa», elemento essencial ao conceito de crime, constitui um limite do critério segundo o qual se determinaria a unidade ou pluralidade de infracções pela unidade ou pluralidade de tipos realizados

III - É a violação concreta das normas na sua função de determinação, precisamente a falta da sua eficácia querida, devida e, portanto, possível no domínio da representação e do processo de motivação do agente, que faz nascer aquele juízo de censura em que se estrutura a culpa.

IV - O índice da unidade, ou pluralidade, de determinações volitivas apenas se pode consubstanciar na forma como o acontecimento exterior se desenvolveu, olhando fundamentalmente à conexão temporal que liga os vários momentos da conduta do agente.

V - Uma pluralidade de factos externamente separáveis deve conformar uma acção unitária quando os diversos actos parciais, que respondem a uma única resolução volitiva, se encontram tão ligados no tempo e espaço que, para um observador não interveniente são percepcionados como uma unidade natural.

VI - O crime por cuja unidade ou pluralidade se demanda é o facto punível e, por conseguinte, uma violação de bens jurídico-penais que integra um tipo legal. A essência de uma tal violação reside no substrato de vida dotado de um sentido negativo de valor jurídico-penal, reside no ilícito típico: é a unidade ou pluralidade de sentidos de ilicitude típica existente no comportamento global do agente submetido á cognição do tribunal que decide, em definitivo, da unidade ou pluralidade de factos puníveis e, nesta acepção, de crimes (…)".

Assim, e para efeitos da análise a que nos propomos poderemos sumariar a questão da seguinte forma:

Verificando-se que determinada conduta pode preencher, prima facie, diversos tipos podemos distinguir entre:

- Concurso legal, aparente ou impuro – em que a conduta do agente apenas formalmente preenche vários tipos de crime, mas, por via de interpretação, conclui-se que o conteúdo dessa conduta é exclusiva e totalmente abrangido ou absorvido por um só dos tipos violados, pelo que os outros tipos devem recuar, não sendo aplicados, podendo os diversos tipos de crime encontrar-se conexionados por diversas relações entre si;
- Especialidade – um dos tipos aplicáveis (tipo especial) incorpora os elementos essenciais de um outro tipo também aplicável abstractamente (tipo fundamental), acrescendo elementos suplementares ou especiais referentes ao facto ou ao próprio agente;
- Consunção – o preenchimento de um tipo legal (mais grave) inclui o preenchimento de outro tipo legal (menos grave) devendo a maior ou menor gravidade ser encontrada na especificidade do caso concreto;
- Subsidiariedade – em que certas normas só se aplicam subsidiariamente, ou seja, quando o facto não é punido por uma outra norma mais grave;
- Facto posterior não punível – os crimes que visam garantir ou aproveitar a impunidade de outros crimes (crimes de garantia ou aproveitamento) não são punidos em concurso efectivo com o crime de fim lucrativo ou de apropriação, salvo se ocasionarem um novo dano ao ofendido ou se dirigirem contra um novo bem jurídico;

- Concurso efectivo, verdadeiro ou puro – em que entre os tipos legais preenchidos pela conduta do agente se não dá uma exclusiva via de qualquer das regras, como acontece com o concurso ideal, mas antes as diversas normas aplicáveis aparecem como concorrentes na aplicação concreta.

Aqui chegados e tendo presente estes vectores tentaremos analisar a relação entre os diversos tipos vertidos na Lei n.º 109/2009 e ainda um outro que é o da burla informática previsto no artigo 221.º do Código Penal.

Vamos mesmo começar por este tipo.

Só se compreende que este tipo esteja no Código Penal se se entender que o bem jurídico protegido pela norma é o património e que o tipo diverge da burla tradicional pelos diferentes meio utilizados na comissão do crime.

Se este não fosse o entendimento mal se compreenderia que a burla informática não fosse senão mais um crime contido na Lei do Cibercrime.

O artigo 221.º do Código Penal dispõe, nos n.ºs 1 e 2 (aqueles que interessam no caso vertente) que:

"1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações."

A relação deste tipo com o da falsidade informática é de especial interesse.

Na falsidade informática visa-se a produção de dados ou documentos não genuínos, mas tal produção terá de ocorrer com intenção de provocar engano nas relações jurídicas.

Na burla informática o agente age com intenção de obter um enriquecimento ilegítimo mediante a interferência no resultado de tratamento de dados, estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento.

Ora, esta interferência da burla pode ocorrer mediante dados falsos obtidos da forma descrita no tipo da falsidade informática e nesse sentido a falsidade seria apenas e só um dos passos necessários à burla.

Poderemos conceber um concurso aparente?

A questão não é nova e o Supremo Tribunal de Justiça, designadamente no Acórdão de Uniformização de Jurisprudência n.º 8/2000. DR 119 SÉRIE I-A de 2000-05-23 reafirmou a posição anteriormente assumida, concluindo que, sendo distintos os bens jurídicos tutelados pelos tipos legais de crime de burla (o património) e de falsificação de documento (a verdade intrínseca do documento enquanto tal) e não se verificando, entre eles, qualquer relação de especialidade, subsidiariedade ou consunção nem se configurando nenhum dos crimes em relação ao outro como facto posterior não punível [. . .] deve continuar a concluir-se que a conduta do agente que falsifica um documento e o usa, astuciosamente, para enganar ou induzir em erro o burlado integra (suposta, naturalmente, a verificação de todos os elementos essenciais de cada um dos tipos), efectivamente, em concurso real, um crime de falsificação de documento e um crime de burla. Por todo o exposto, não se vê qualquer razão para que a doutrina constante do acórdão fundamento deva ser alterada. Impõe-se, contudo, fazer uma actualização na referência aos artigos hoje vigentes. Conclui a mesma decisão no sentido de uniformizar a jurisprudência na esteira do entendimento anteriormente seguido decidindo que:

> «No caso de a conduta do agente preencher as previsões de falsificação e de burla do artigo 256.º, n.º 1, alínea a), e do artigo 217.º, n.º 1, respectivamente, do Código Penal, revisto pelo Decreto-Lei n.º 48/95, de 15 de Março, verifica-se concurso real ou efectivo de crimes.»

Já posteriormente o mesmo Supremo Tribunal de Justiça e quanto à mesma questão de concurso firmou novo AUJ em 05.06.2013 (DR, I SÉRIE, 131, 10.07.2013, P. 4015) onde considerou que:

> *"A alteração introduzida pela Lei 59/2007 no tipo legal do crime de falsificação previsto no artigo n.º 256 do Código Penal, estabelecendo um elemento subjectivo especial, não afecta a jurisprudência fixada nos acórdãos de fixação de jurisprudência de 19 de Fevereiro de 1992 e 8/2000 de 4 de Maio de 2000 e, nomeadamente, a interpretação neles constante de que, no caso de a conduta do agente preencher as previsões de falsificação e de burla do artigo 256.º, n.º 1, alínea a), e do artigo 217.º, n.º 1, do mesmo Código, se verifica um concurso real ou efectivo de crimes".*

Esta decisão não foi pacífica diga-se.

Mas esta é, até mais ver, a posição do Supremo Tribunal de Justiça a qual merece acatamento por parte dos Tribunais (dentro dos parâmetros do artigo 445.º, n.º 3, do Código do Processo Penal).

Poderemos transpor tal jurisprudência para o ambiente digital por assim dizer?

Creio que não, pelas razões que passarei a expor.

O ambiente em que a acção típica decorre é diferente.

O falsificador informático não age para a obtenção pura e simples do dado viciado. A adulteração do dado ou do tratamento informático de dados com o fim de conseguir um documento não genuíno não é um fim em si. O falsificador pretende que este seja utilizado ou considerado para finalidade juridicamente relevantes como se genuíno fosse.

E isto é um passo para a burla. A falsificação informática pode ser um dos momentos da burla.

A plena compreensão do elemento subjectivo especial da falsificação [a intenção de provocar engano nas relações jurídicas] permite aproximar, na perspectiva do bem jurídico protegido, este crime da burla.

Também a burla informática comporta um elemento subjectivo especial (para além do dolo) – a intenção de enriquecimento ilegítimo –, cuja configuração tem pontos de convergência com o da falsificação (embora o benefício almejado nesta não tenha de ser patrimonial). Por isso, recorrendo à lapidar fórmula preconizada por *Figueiredo Dias* para definir o concurso aparente, legal ou impuro de crimes, entendo ser defensável que «o conteúdo ou a substância criminosa do comportamento é esgotantemente abarcado pela aplicação ao caso de um só dos tipos violados» (Direito Penal, Sumários e Notas das Lições do Prof. Doutor Jorge Figueiredo Dias ao 1.º ano do Curso Complementar da Faculdade de Direito da Universidade de Coimbra de 1975-1976, pp. 102 e 103…). Deste modo, pode concluir-se que, em determinados casos, se verifica uma consunção, sendo o agente punível apenas por burla.

Nesta perspectiva, a falsificação, se consumida pela burla, passaria a ser ponderada como circunstância (agravante) geral na determinação da pena concreta, à semelhança do que sucede, por exemplo, quanto à violação de domicílio no âmbito do furto qualificado.
Esta questão não é pacifica desde logo porque as penas a aplicar são muito diferentes em ambas as situações.

Na verdade, situações existem (designadamente as do n.º 2 a 5 do artigo 3.º, da Lei n.º 109/2009, de 15.10) em que a medida abstracta da pena da falsificação é superior á da pena simples da burla informática prevista no artigo 221.º do Código Penal.

Nestas situações, em que a pena abstracta da falsificação é superior à da burla, estamos em crer que o concurso é tão só aparente pois que a pena da burla, só por si, não é capaz de satisfazer os fins do artigo 40.º do Código Penal.

A solução passará, pois, pela aplicação da pena que melhor defende os interesses preconizados no artigo 40.º do Código Penal, ou seja, nunca subsumir a conduta a um tipo que pune menos do que o conjunto dos tipos em presença. Dito de outra forma, para se considerar um concurso aparente teremos de considerar, sempre, que o tipo que permanece consegue acomodar dentro de si a condenação pelos actos do tipo consumido.

Uma outra questão prende-se com o tempo. Na verdade, para se poderem distinguir acções terá o intérprete de conceber que existem acções diferentes. Se se falsificam dados e estes imediatamente correm num sistema informático dificilmente conseguiremos dizer que houve duas resoluções distintas até porque na falsidade informática só é relevante a falsificação que

se destine a que os dados sejam considerados ou utilizados para finalidades juridicamente relevantes.

A questão posta pode também sê-lo no que tange à falsificação e à contrafacção de cartões e outros dispositivos de pagamento (artigo 3.º-A da Lei n.º 109/2009 de 15 de Setembro).

Na verdade, a contrafacção pode ser mecânica mas nos tempos que correm será muito certamente feita na base da adulteração dos dados e aí a questão volta a colocar-se.

Chamo também a atenção para a relação entre os crimes previstos nos artigos 4.º e 5.º, da Lei n.º 109/2009, de 15 de Setembro.

É necessário ter muito cuidado na apreciação do artigo 4.º (dano relativo a programas) e estabelecer a sua relação com o crime de sabotagem informática previsto no artigo 5.º da Lei n.º 109/2009 de 15.09.

É que no preceito em apreço são danificados dados ou programas com intuitos lucrativos ou de causar prejuízo e no artigo 5.º são danificados dados, programas ou sistemas informáticos com a intenção de os entravar. Quer num preceito, quer noutro, os meios podem ser idênticos, havendo diferenças ao nível do *animus* do agente.

A pessoa lesada tem interesse não só em que os programas ou dados registados no computador permaneçam inteiros ou intactos, ou integrais em sentido quantitativo, mas também que permaneçam intactos em sentido qualitativo, quer dizer que não se deteriorem.

Assim o tipo legal em causa visa assegurar uma protecção análoga à que gozam os bens corpóreos contra danos causados intencionalmente. No fundo, trata-se dos "danos de um programa ou ficheiro", em tudo semelhantes aos do artigo 212.º do Código Penal. No entanto surge-nos aqui este específico tipo de danos dada a natureza dos mesmos, incidência sobre bens incorpóreos em que a lesão se faz não sobre a substância de um objecto, mas sobre a informação contida em dados ou programas informáticos, que podem diminuir o seu uso. Deste modo temos para nós que este tipo é especial em relação ao do artigo 212.º do Código Penal.

O crime de sabotagem informática distingue-se do crime de dano informático em face do objecto da acção típica, dado que aqui estamos perante uma lesão do próprio sistema de comunicação e não só perante uma lesão dos dados ou programas informáticos.

Igualmente o elemento subjectivo é diferente, dado que aqui o que está em causa é a intenção de entrave ou perturbação do funcionamento de um sistema informático ou de comunicação de dados à distância.

Por outro lado, entendemos que, dado que neste tipo se podem incluir condutas que consistam na alteração de programação de dados, através da viciação dos mesmos, também existe uma forma de falsificação de dados informáticos, os quais quando sejam possuidores de características de documentos, fazem com que a conduta do agente deva ser punida em concurso aparente entre este artigo e o artigo 3.º.

É que a realização do próprio artigo 5.º pressupõe necessariamente a falsificação de um documento informático.

E na verdade aqui o crime de sabotagem informática acomoda perfeitamente no seio a inclusão da falsificação informática como agravante. Melhor ainda: pressupõe a mesma, porquanto elemento do tipo.

A sabotagem informática surge também em relação especial com o crime de acesso ilegítimo.

Na verdade, este tipo é complementar da sabotagem informática, uma vez que se traduz numa protecção antecipada e indirecta da mesma, existindo entre as condutas um concurso aparente (para além de que acaba por ser um tipo residual dentro da própria lei, dado que para a prática de qualquer das condutas incriminadas pela mesma lei, acaba sempre por haver necessidade de acesso a um sistema ou rede informática).

Em suma, este crime está sempre em concurso aparente com os demais, sendo consumido sempre que a conduta exigida para preenchimento do outro tipo seja um acesso ilegítimo.

A intercepção ilegítima tem uma relação com o acesso ilegítimo sendo este apenas o início daquela.

Na intercepção visa-se conhecer o conteúdo de transmissões de dados que circulam num sistema. Para tal é necessário aceder (ilegitimamente) ao sistema.

Assim, a relação entre estes dois tipos é a de um concurso aparente sendo o acesso consumido pela intercepção.

Quanto ao artigo 8.º A (aditado pelo Decreto-Lei n.º 125/2025, de 04 de Dezembro):

O que se encontra no artigo 8.º A da Lei do Cibercrime é uma causa de exclusão da culpa, como parece resultar das alusões recorrentes a intenção única de contribuir para salvaguardar a segurança do ciberespaço, ao propósito de actuação desconectada de qualquer intuito lucrativo e de obtenção de vantagem patrimonial e, tendo por referência as causas de exclusão da culpa classicamente previstas no Código Penal, será, porventura, com o estado de necessidade desculpante que guarda maior similitude.

O estado de necessidade (em sentido amplo) em direito penal, reporta-se a situações que não são de legítima defesa, mas nas quais só é possível salvar certos interesses ou valores ameaçados ou em risco de perda ou de lesão, à custa do sacrifício de outros interesses juridicamente protegidos, traduzindo esse sacrifício um comportamento que preenche um tipo legal de crime.

Nos termos do artigo 35.º, n.º 1, do Código Penal, «*age sem culpa quem praticar um facto ilícito adequado a afastar um perigo actual, e não removível de outro modo, que ameace a vida, a integridade física, a honra ou a liberdade do agente ou de terceiro, quando não for razoável exigir-lhe, segundo as circunstâncias do caso, comportamento diferente*».

A exclusão da culpa decorre de, nas circunstâncias concretas do facto, não ser razoável exigir do agente um comportamento diferente.

A punibilidade é afastada, em virtude de «*considerações retiradas das circunstâncias concretas do facto e do seu agente, que fazem que in casu não seja razoável exigir dele outro comportamento*»; apesar do ilícito-típico praticado demonstra-se «a persistência no agente de uma atitude de fidelidade do direito que aponta a fundamentação do facto numa atitude pessoal juridicamente desvaliosa ou em qualidades juridicamente desvaliosas da sua personalidade» (Figueiredo Dias, Sobre o Estado Actual da Doutrina do Crime, 2ª parte, Sobre a construção do tipo-de-culpa e os restantes pressupostos da punibilidade, Revista Portuguesa de Ciência Criminal, Ano 2, 1.º, pág. 28).

São pressupostos do estado de necessidade desculpante:

Verificar-se uma situação de perigo actual para bens jurídicos de natureza pessoal (vida, integridade física, honra e liberdade) do agente ou de terceiro.

O facto ilícito praticado tem de ser "adequado", ou seja, idóneo a afastar o perigo que não seria remível por outro modo.

Para além destes elementos objectivos relacionados com o perigo, o bem jurídico ameaçado e a adequação do facto é necessário que o juiz verifique que não era razoável exigir do agente, segundo as circunstâncias do caso, comportamento diferente.

O facto ilícito praticado tem de ser “adequado”, ou seja, idóneo a afastar o perigo que não seria remível por outro modo.

Para além destes elementos objectivos relacionados com o perigo, o bem jurídico ameaçado e a adequação do facto é necessário que o juiz verifique que não era razoável exigir do agente, segundo as circunstâncias do caso, comportamento diferente.

É ainda indispensável que o agente pratique a acção para determinar com ela a preservação do bem jurídico ameaçado, isto é, o «animus salvandi», o que bem se compreende pois está em causa a prática de um facto ilícito e, por conseguinte, juridicamente desaprovado (Figueiredo Dias, Direito Penal, Parte Geral, Tomo I, 2.ª edição, pág. 618).

O estado de necessidade desculpante pode reconduzir-se, assim, ao princípio da inexigibilidade de um comportamento ajustado à norma.

E é precisamente isto, com as devidas adaptações, que o artigo 8.º A da Lei do Cibercrime também consagra ao erigir a segurança do ciberespaço a bem jurídico de valor maior, cuja preservação se só puder ser conseguida à custa de comportamentos integradores dos crimes de acesso ilegítimo e de intercepção ilegítima previstos, respectivamente, nos artigos 6.º e 7.º, implica que estes crimes deixam de ser puníveis, uma vez verificados cumulativamente os demais pressupostos enumerados no citado artigo 8.º A.

Também ali se encontra o «animus salvandi», quer com a alusão à intenção de contribuir para assegurar a integridade do ciberespaço e a segurança das comunicações e da regular transmissão e circulação de dados de informação, quer com o requisito negativo de que o agente não procure qualquer vantagem patrimonial, assim como o princípio da proporcionalidade, na acepção do artigo 18.º, n.º 2, da Constituição da República Portuguesa (necessidade, adequação e proporcionalidade), visto que estão aqui em causa vários direitos, liberdades e garantias fundamentais, como seja, o direito à reserva da intimidade da vida privada, ao segredo e inviolabilidade das comunicações, bem como a protecção dos dados pessoais dos utilizadores dos vários domínios do ciberespaço, que expressamente, vem exigida na nas alíneas d) e e) do n.º 2 e concretizada, pela negativa, através de múltiplos índices factuais concretos que se encontram descritos nas alíneas a) a g) do n.º 3 que, por corresponderem a condutas objectivas, elas próprias integradoras de outros cibercrimes como os de falsidade informática, burla informática ou, pelo menos, de modos de execução típica destes crimes, afastam a aplicabilidade desta causa de exculpação.

Uma outra questão que pode sopesar-se, dependendo das circunstâncias do caso, é a de na eventualidade, de não estarem cumulativamente verificados todos os pressupostos enunciados no artigo 8.º A de que depende a ausência de punição, mas apenas alguns, se haverá lugar à atenuação especial da pena, nos termos do regime geral contido nos artigos 72.º e 73.º do Código Penal.

Sem, na verdade, pretender apresentar uma posição final e definitiva, estou em crer que não se pode chamar à colação a figura da atenuação especial pois que a mesma depende da verificação de uma atenuação acentuada da ilicitude, da culpa ou das necessidades da pena (artigo 72.º, n.º 1, do Código Penal). Esta diminuição é analisada caso a caso e não se poderá dizer, *ab initio* que a presença de alguns dos pressupostos do artigo 8.º A e a ausência de outros só por si (ou por si) determinem a atenuação especial.

Dito isto, o artigo 8.º A convoca a enumeração de um conjunto de práticas cujo conteúdo se deve ter por assente.

Assim o preceito menciona técnicas de engenharia social, a *phishing* e suas variantes.

A título ilustrativo deixamos aqui alguns conceitos (apelando ao constante do Acórdão da Relação de Lisboa de 15.07.2024, tirado no Processo n.º 670/20.3JGLSB.L1, já mencionado).

Menciona o preceito o *phishing*.

O *phishing* corresponde a «um procedimento de cariz tecnológico que se alia a técnicas de Engenharia Social (conjunto de práticas que exploram a confiança dos utilizadores, sem necessidade de emprego de qualquer meio técnico, aproveitando-se da dificuldade dos mesmos em acompanhar os progressos informáticos e de compreenderem, por isso, a sua potencialidade para a lesão de bens pessoais e patrimoniais essenciais.
Estas técnicas tomam em atenção o facto de o elemento mais fraco de qualquer sistema de segurança de informação ser o próprio ser humano, devido aos seus traços comportamentais e psicológicos que o tornam mais susceptíveis a estes ataques. É, assim, uma ferramenta de

exploração das falhas humanas em organizações físicas ou jurídicas) com o intuito de obter informação pessoal e confidencial – e não apenas credenciais de identificação –, daqueles que tiram proveito das múltiplas plataformas online.

> *«Por isso, este tipo de ataque inicia-se tradicionalmente com um e-mail forjado através do qual os criminosos se fazem passar pelas organizações legítimas, detentoras das informações pretendidas (servindo-se das suas designações comerciais, logótipos, slogan's, endereços de e- mail, etc.), que, com justificações mais ou menos plausíveis visam os seguintes objetivos:*
>
> *«Furto de credenciais de acesso a sites na web (como Hotmail, Gmail, eBay), que, não raro, servem de base a mecanismos em linha de realização de transferências monetárias;*
>
> *«Furto de credenciais de acesso a serviços bancários (Net-banco);*
>
> *«Acesso aos detalhes de cartões de crédito;*
>
> *«Obtenção de moradas e endereços de e-mail, já que estas são informações transacionáveis, nomeadamente para empresas com fins publicitários;*
>
> *«Furto de segredos e outros documentos confidenciais (podendo falar-se a este propósito de Spear Phishing).*
>
> *«Distribuição de botnets e agentes DDoS» (Joana Margarida Andrade Gonçalves, Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património, Outubro de 2015, p. 19, in https://core.ac.uk/download/pdf/55640946.pdf).*

Os estratagemas de *smishing* e *vishing* constituem estratagemas de captação de informações confidenciais e sensíveis que as vítimas compartilham voluntariamente acerca de si próprias e dos seus bens, fruto de tomadas de decisão manipuladas e induzidas pelos agentes a partir de três factores fundamentais: confiança, contexto e emoção.

Com efeito, fazendo-se passar por pessoas com determinadas funções ou qualidades associadas a organizações legítimas e reconhecidas como tal, por isso, confiáveis, os agentes da criminalidade informática diminuem os riscos de descrédito ou cepticismo das vítimas, sendo certo que as comunicações através de mensagens de texto SMS, sendo um canal de comunicação mais pessoal, também diminuem naturalmente as defesas da pessoa contra ameaças (confiança) (Pedro Verdelho, in Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade De Informação, Volume VIII, 407/419: Maria Raquel Guimarães, in Cadernos de Direito Privado, n.º 41, Janeiro/Março de 2013; Mark A Fox, Phishing, Pharming and Identity Theft in The Banking Industry, in Journal of international banking law and regulation, editado por Sweet and Maxwel (2006), Issue 9, 548/552; Roberto Flor, Phishing, Identity Theft e Identity Abuse. Le Prospecttive Applicative Del Diritto Penale Vigente, in Revista Italiana di Diritto e Procedura Penale, Fasc 2/3-Aprile-Settembre 2007, 899/9446).

Isso, associado à criação ou utilização de uma situação verosímil, permite ao invasor cibernético um disfarce credível e eficiente. A mensagem parece personalizada, o que ajuda a anular qualquer suspeita de que possa ser spam (contexto), partindo da constatação de que a generalidade das pessoas tende a acreditar que os seus telemóveis são mais seguros do que os computadores, logo, mais imunes a ataques do tipo *phishing*.

A confiança e o contexto interligados e somados a uma determinada emoção - de medo, ou de risco de perda dos bens e valores, ameaças de encerramento imediato da conta, de instauração de acção judicial, promessas de grandes recompensas, prémios em dinheiro ou ofertas exclusivas que exigem tomadas de decisão instantânea, interlocutores que fingem gentileza ou afirmam ter uma conexão pessoal, tentando diminuir as defesas, a insistência no sigilo desencorajando o destinatário de consultar outras pessoas ou verificar sua legitimidade - tendem a anular a serenidade e o pensamento crítico da vítima e a precipitar tomadas de decisão determinadas pelo agente do crime.

Estes meios enganosos e fraudulentos de induzir os destinatários, pessoas singulares ou colectivas, a partilharem com os agentes do crime informações pessoais e outros detalhes confidenciais ou a clicar em links que levam a sites enganosos ou downloads de software malicioso, distinguem-se pelos meios de comunicação utilizados: SMS, no caso do *smishing*, chamadas telefónicas, no caso do *vishing* e e-mails, no caso do *phishing*.

> *«O ataque de SMiShing, variante do phishing, como a própria nomenclatura indica (-shing), tem como objetivo "levar o utilizador a fornecer informação pessoal", através de SMS dos telemóveis, designadamente ser usado enquanto estratégia para "enganar" o recetor da mensagem a transferir dinheiro da sua conta bancária. Segundo um estudo, prevê-se que todos os dias, 1 em 20 utilizadores clique, inadvertidamente, em links de phishing nos seus dispositivos android.*
>
> *«(…) O vishing, como o próprio nome indica, é a conjugação entre "voice" (voz) e "phishing" que utiliza engenharia social sobre o sistema de telefonia. Portanto, o vishing visa o ataque através de PSTN, usando mensagens de voz para obtenção ilícita de dados sigilosos, como dados bancários e para eventuais roubos de identidade, tal como sucede no phishing.*
>
> *«Com efeito, uma conversação de telefone em tempo real aumenta significativamente, a eficácia de engenharia social, o que não sucede nos casos dos e-mails por constituírem uma ferramenta assíncrona, e por terem de ser abertos e lidos deixam menos margem de ataque aos atacantes para atrair as vítimas.*
>
> *«À dissemelhança do phishing, é inerentemente mais difícil de analisar o vishing por ser de difícil rasto.*
>
> *«Como se processa este ataque? O agente do crime tem acesso a um número indeterminado de números de telefones. Quando a vítima atende o telefone ouve uma gravação automática que a informa que a sua conta bancária foi comprometida, seguindo-se a informação de que terá que ligar para um outro número gratuito a fim de*

redefinir as suas configurações de segurança. Depois ouve uma outra mensagem automática que solicita o número da conta bancária da vítima e outros dados pessoais através do teclado do telefone.» (Ana Helena França Azevedo, Burlas Informáticas: Modos de Manifestação, Janeiro de 2016, p. 75-77, in https://repositorium.sdum.uminho.pt/bitstream/1822/44510/1/Ana%20Helena%20Fran%C3%A7a%20Azevedo.pdf *).*

Quanto ao *SPOOFING*:

O *spoofing* é uma técnica de falsificação digital usada para enganar utilizadores e sistemas, fazendo com que pareça que a comunicação vem de uma fonte confiável.

Esse tipo de ataque pode ser usado para apropriação ilícita de dados, invasões e disseminação de *malware*, entre outros objectivos maliciosos.

Sobre a definição de *Spoofing* (retirado do site Tek notícias in h ttps://tek.sapo.pt/how- to/artigos/spoofing-o-que-e-e-como-se-proteger-de-chamadas-falsas-do-banco-ou-das-financas/):

«É uma técnica de falsificação de identidade digital é um tipo dos tipos de ataque que está cada vez mais a ser utilizado em Portugal, segundo alerta a ANACOM, a Autoridade Nacional de Comunicações. O termo spoofing vem do inglês e significa, em traços largos, "enganar" ou "imitar".

«O spoofing pode surgir de formas muito distintas. Na sua variante telefónica, os criminosos manipulam o identificador de chamadas para que o número apresentado no ecrã pareça ser o de uma entidade legítima. Por essa razão é normal a aplicação de telefone do seu smartphone muitas vezes identificar a chamada como sendo do seu banco, da operadora de telecomunicações, da Segurança Social, das Finanças ou até mesmo da PSP.

«Por email, a técnica envolve falsificar o remetente para que a mensagem pareça vir de uma empresa ou de serviço fidedigno. Neste caso, o endereço pode ter diferenças subtis, muitas vezes quase impossíveis de detectar à primeira vista, como a substituição de uma letra por outra visualmente semelhante. Existe ainda o spoofing de sites, em que é criada uma cópia quase perfeita de uma página legítima, com o único propósito de capturar os dados de acesso do utilizador.

«Em todos os casos, o elemento comum é sempre a urgência da ação. Os criminosos criam pressão para que a vítima aja sem pensar. Inventam situações como o possível bloqueio da sua conta bancária, a existência de uma encomenda retida, ou uma tentativa de acesso suspeita a algum serviço ou plataforma. Esta pressão é aplicada deliberadamente, pois quanto menos tempo a vítima tiver para reflectir, maior a probabilidade de cair no golpe.

«Como reconhecer uma tentativa de spoofing?

«Há vários sinais de alerta que devem ser tidos em conta para não cair nesta burla. Pedidos inesperados de dados pessoais, códigos de autenticação ou transferências bancárias são sempre pedidos suspeitos, independentemente de quem pareça estar a pedir. Nenhuma instituição financeira, órgão público ou empresa solicita palavras-passe ou códigos de segurança por telefone, SMS ou email.

«Mensagens com erros ortográficos, pressão para agir "agora mesmo" ou links que não correspondem exactamente ao site oficial são igualmente indicadores de fraude. Nos emails, vale a pena verificar o endereço completo do remetente, não apenas o nome que aparece. Esse endereço "real" costuma estar entre parênteses angulares, quase sempre finalizados com domínios estranhos, e muito diferentes do domínio oficial da entidade.

«O que fazer se suspeitar de *spoofing*?

A ANACOM é clara nas recomendações dadas. Em caso de contacto, não clique em links, não partilhe dados e não confirme qualquer informação indicada. Se receber uma chamada suspeita, desligue. Se receber uma mensagem duvidosa, apague-a. Em ambos os casos, contacte diretamente a entidade através do número ou endereço oficial, e nunca a partir do contacto que recebeu.

«Deverá confirmar sempre pelo canal oficial da entidade que, supostamente, o contactou. Se tiver dúvidas sobre um email, não responda nem clique em nenhum link. Aceda ao site da entidade digitando o endereço directamente no browser. Verifique se o endereço utiliza um acesso seguro, ou seja, se começa por "https://” e se existe o ícone de cadeado junto ao URL, sinais de que a ligação é segura.

O termo *spoofing* está a tornar-se cada vez mais comum no que diz respeito a ataques cibernéticos, uma vez que é uma técnica que pode ser usada para *phishing*.

O principal ponto-chave de um ataque de *spoofing* é que a mensagem aparenta ter como proveniência uma fonte segura, levando alguém a ultrapassar uma barreira de defesa mental. Ou seja, este tipo de ataque acontece quando alguém se faz passar por outra pessoa, por norma alguém que nos é próximo ou até um superior hierárquico, na tentativa de ganhar a nossa confiança, obter acesso aos nossos sistemas ou incentivar à realização de determinada acção, com o objectivo de obter acesso ilegítimo a recursos que podem, por exemplo resultar em perdas financeiras.

Os ataques de *spoofing* assumem diversos tipos de falsificação da origem da comunicação, como: correio eletrónico, de identificador de chamadas telefónicas, de mensagens de texto ou até de coordenadas de GPS.

Os métodos mais recorrentes de *spoofing* são através do envio de um *e-mail* ou através de uma chamada telefónica.

Na prática, os atacantes enviam um e-mail com uma hiperligação de *phishing*, levando a vítima para um *website* que se assemelha a um outro que costuma visitar – por exemplo, a página inicial de um *website* do seu banco.

A chamada telefónica difere um pouco, mas o objectivo é o mesmo, no sentido em que a vítima recebe uma suposta chamada do seu banco e o ciberatacante faz-se passar por alguém que trabalha nesse banco, fazendo com que a vítima forneça os seus dados de identificação e as respectivas passwords.

Este tipo de ataque é uma crescente preocupação para o ecossistema de cibersegurança, uma vez que está a evoluir e os atacantes estão a ser cada vez mais minuciosos na forma como atacam. É importante saber quais são as melhores práticas de cibersegurança para se poder proteger e prevenir de ataques de *spoofing*.

Bibliografia:

- **Bravo, Rogério –** Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na Ciber-Convenção in https://www.academia.edu/2039178/O_Crime_de_Acesso_Ilegi_timo_na_Lei_da_Criminalidade_Informa_tica_e_na_CiberConvencao (consultado em 14.06.2025).

- **Dias Pereira, Alexandre Libório** – Internet, Direito de Autor e Acesso Reservado, As Telecomunicações e o Direito na Sociedade da Informação, Instituto Jurídico da Comunicação, Faculdade de Direito da Universidade de Coimbra, Coimbra, 1999.

- **Dias Pereira, Alexandre Libório** – Comércio Electrónico na Sociedade da Informação: Da Segurança Técnica à Confiança Jurídica, Livraria Almedina, Coimbra, 1999.

- **Faria Costa, José Francisco** – Direito Penal da Comunicação, Alguns Escritos, Coimbra Editora, Coimbra, 1998.

- **Faria Costa, José Francisco e Moniz, Helena** – Algumas Reflexões sobre a Criminalidade Informática em Portugal, Boletim da Faculdade de Direito de Coimbra, n.º 73, 1997.

- **Figueiredo Dias,** Comentário Conimbricense ao Código Penal, tomo II, Coimbra Editora, Coimbra, 1999.

- **Januário Lourenço, Pedro Miguel** – Criminalidade Informática no Ciberespaço, Estudos de Direito da Comunicação, Instituto Jurídico da Comunicação, Faculdade de Direito da Universidade de Coimbra, Coimbra, 2002.

- **Lopes da Rocha, Manuel** – Direito da Informática nos Tribunais Portugueses 1990 – 1998, Edições Centro-Atlântico, 1999.

- **Lopes da Rocha, Manuel** – A Lei da Criminalidade Informática (Lei 109/91 de 17 de Agosto)

Génese e Técnica Legislativa, Revista de Legislação, 8, 1993.

– **Marques, Garcia** – "A Lei 10/91 de 29 de Abril – Lei de Protecção de dados pessoais face à informática", Documentação e Direito Comparado, 47.º e 48.º, 1991.

– **Marques, Garcia e Martins, Lourenço** – Direito da Informática, Livraria Almedina, Coimbra, 2000.

– **Moura e Silva, Miguel** – Protecção de Programas de Computador na Comunidade Europeia, Revista Direito e Justiça, Vol. VIII, 1993.

– **Nunes, Duarte Rodrigues** – Os crimes previstos na Lei do Cibercrime, Gestlegal, Lisboa, 2024.

– **Oliveira Ascensão** – Estudos sobre Direito da Internet e da Sociedade Informação, Livraria Almedina, Coimbra, 2001.

– **Oliveira Ascensão** – A protecção Jurídica dos programas de computador, R.O.A., ano 50.º, I, Abril, 1990.

– **Pereira, Joel Timóteo Ramos** – Direito da Internet e Comércio Electrónico, Quid Juris ? – Sociedade Editora, Lisboa, 2001.

Vídeo da intervenção

https://educast.fccn.pt/vod/clips/2pzj8dspkp/streaming.html?locale=pt

2. ANÁLISE PRÁTICA DOS ARTIGOS 15.º E 17.º DA LEI DO CIBERCRIME[1]

Valter Alves*

Vídeo da intervenção

https://educast.fccn.pt/vod/clips/2pzj8dsqs4/streaming.html?locale=pt

[1] Comunicação do autor no Seminário «Cibercrime e e-evidence», realizado em Lisboa, em 20 de abril de 2026, no Centro de Estudos Judiciários.

* Procurador da República em funções na 7.ª Secção do DCIAP.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3. COOPERAÇÃO JUDICIÁRIA INTERNACIONAL EM MATÉRIA PENAL E PROVA DIGITAL: QUADRO LEGAL VIGENTE E DESENVOLVIMENTOS RECENTES E FUTUROS[1]

Antero Taveira*

Sumário Executivo

(**1**) A obtenção de prova digital em contexto transfronteiriço constitui um dos desafios centrais do processo penal contemporâneo, impondo adaptações profundas aos instrumentos tradicionais de cooperação judiciária internacional.

(**2**) O quadro normativo aplicável é composto por camadas sobrepostas de instrumentos – nacionais, convencionais e da União Europeia – cada um com lógicas, âmbitos e destinatários distintos.

(**3**) O pacote legislativo europeu de *e-evidence* (Regulamento (UE) 2023/1543 e Diretiva (UE) 2023/1544), com aplicação a partir de agosto de 2026, representa uma mudança de paradigma ao permitir o envio direto de ordens de produção e conservação a prestadores de serviços estabelecidos noutro Estado-Membro.

(**4**) O Segundo Protocolo Adicional à Convenção de Budapeste introduz mecanismos simplificados de cooperação direta com entidades privadas para além do espaço da União Europeia.

(**5**) A Convenção das Nações Unidas contra o Cibercrime, assinada em outubro de 2025, alarga a ambição deste quadro à escala global.

(**6**) Persistem obstáculos relevantes, de natureza técnica, processual e de direitos fundamentais, cuja superação exige formação especializada, investimento em infraestruturas digitais e diálogo estruturado entre todos os atores envolvidos.

Resumo: O presente artigo analisa o quadro normativo da cooperação judiciária internacional em matéria de recolha de prova digital, percorrendo as soluções previstas na Lei do Cibercrime portuguesa, na Convenção de Budapeste e no seu Segundo Protocolo Adicional, no pacote legislativo comunitário sobre prova eletrónica (*e-evidence*) e na recente Convenção das Nações Unidas contra o Cibercrime. Para além da enunciação dos instrumentos vigentes e dos mecanismos processuais que contemplam, o artigo identifica os principais problemas práticos que se colocam às autoridades judiciárias e aos prestadores de serviços, com especial atenção às questões que permanecerão em aberto após a aplicação plena do Regulamento (UE) 2023/1543 em agosto de 2026.

Palavras-chave: Cibercrime; Prova digital; Cooperação judiciária internacional; Pacote *e-evidence*; Convenção de Budapeste; Ordem europeia de produção; Regulamento (UE) 2023/1543.

***Abstract**: This article examines the legal framework governing international judicial cooperation in the collection of e-evidence, covering the solutions laid down in the Portuguese Cybercrime Act, the Budapest Convention and its Second Additional Protocol, the EU e-evidence legislative package, and the recently adopted United Nations Convention against Cybercrime. Beyond an account of the instruments in force and the procedural mechanisms they provide, the article identifies the main practical challenges facing judicial authorities and service providers, with particular attention to the issues that will remain open after the full entry into force of Regulation (EU) 2023/1543 in August 2026.*

***Keywords**: Cybercrime; Digital evidence; International judicial cooperation; E-evidence package; Budapest Convention; European Production Order; Regulation (EU) 2023/1543.*

Índice:

Vídeo da intervenção

[1] Artigo desenvolvido e ampliado a partir da comunicação apresentada pelo autor no Seminário «Cibercrime e e-evidence», realizado em Lisboa, em 20 de abril de 2026, no Centro de Estudos Judiciários. O texto ora publicado representa uma elaboração académica autónoma da apresentação original, com desenvolvimento doutrinário, análise de fontes primárias e notas de referência bibliográfica que não constavam da comunicação oral e respetivo suporte. Contempla, igualmente, uma atualização, em face da entretanto surgida Proposta de Lei n.º 83/XVII/1.ª..

* Procurador da República, Docente no Centro de Estudos Judiciários.

I. INTRODUÇÃO: A ESPECIFICIDADE DA PROVA DIGITAL EM CONTEXTO TRANSFRONTEIRIÇO

De acordo com dados recolhidos pela Comissão Europeia junto de autoridades policiais e judiciais de vários Estados-Membros, a prova eletrónica é relevante em cerca de 85% das investigações criminais e, em aproximadamente dois terços desses casos, a obtenção da mesma exige um pedido dirigido a prestadores de serviços sediados noutra jurisdição.[2] Estes números, abundantemente citados no debate legislativo europeu, ilustram com clareza a inadequação dos instrumentos de cooperação judiciária penal tradicionais face à natureza intrinsecamente transfronteiriça da prova digital.

Como é sabido, a prova digital apresenta características que a distinguem profundamente da demais prova, dir-se-ia material ou clássica.

A sua volatilidade – suscetibilidade de eliminação em micro-segundos – contrasta com a habitual morosidade dos mecanismos convencionais de auxílio judiciário mútuo.

A sua ubiquidade – os dados de um utilizador em Lisboa podem estar armazenados em servidores distribuídos por vários países, ou em clouds cuja localização física não é sequer facilmente determinável3 – torna inadequado qualquer enquadramento jurídico assente exclusivamente no princípio da territorialidade.

Para além disso, a elevada sensibilidade desses dados, que frequentemente incluem comunicações privadas, dados de localização e informação financeira, convoca ainda as mais exigentes garantias de direitos fundamentais.

A complexidade não se esgota no plano técnico. De um ponto de vista jurídico, as investigações que envolvem prova digital de natureza transfronteiriça impõem uma navegação simultânea em múltiplas camadas normativas – o direito nacional, as convenções internacionais bilaterais e multilaterais, o direito da União Europeia – cada uma com a sua teleologia, os seus destinatários, as suas formalidades e os seus mecanismos de controlo.

O presente artigo propõe-se, de alguma forma, mapear esse quadro normativo, partindo das disposições da Lei do Cibercrime, passando pela Convenção de Budapeste e seu Segundo Protocolo Adicional, pelo novel pacote legislativo comunitário relativo à recolha de e-

---

[2] Comissão Europeia, Documento de Trabalho dos Serviços da Comissão – Avaliação de Impacto, SWD(2018) 118 final, de 17 de abril de 2018, que acompanha a proposta de Regulamento relativo às ordens europeias de produção e de conservação de provas eletrónicas e a proposta de Diretiva relativa à nomeação de representantes legais, p. 13. Disponível em:
EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018SC0118.
Os dados foram recolhidos através de inquéritos a autoridades policiais e judiciais de vários Estados-Membros e têm sido amplamente citados como fundamento da intervenção legislativa europeia, sendo reproduzidos na Exposição de Motivos da Proposta de Lei n.º 83/XVII/1.ª.

[3] Sobre os desafios colocados pelas *clouds* à cooperação internacional v. Bert-Jaap Koops / Morag Goodwin, «Cyberspace, the Cloud, and Cross-Border Criminal Investigation, The limits and possibilities of International Law» Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, December 2014 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=269826).

evidence, e chegando até à recentemente adotada Convenção das Nações Unidas contra o Cibercrime. Para além da enunciação dos instrumentos, procura identificar as tensões e os problemas práticos que subsistem e que, em alguns casos, subsistirão mesmo após a plena entrada em vigor dos instrumentos mais recentes.

II. O ENQUADRAMENTO NACIONAL: A LEI DO CIBERCRIME

1. Âmbito e estrutura

A Lei n.º 109/2009, de 15 de setembro[4]– a Lei do Cibercrime, doravante, LCC –, constitui o pilar fundamental do quadro normativo nacional nesta matéria. Aprovada em transposição da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e em execução das obrigações decorrentes da ratificação da Convenção de Budapeste – cujas disposições mais relevantes serão infra analisadas – veio estabelecer um conjunto de tipos legais de crimes informáticos e simultaneamente definir o regime processual aplicável à investigação de crimes cometidos por meios informáticos ou que envolvam a recolha de prova em formato digital.

O seu artigo 11.º delimita o âmbito de aplicação das disposições processuais[5], abrangendo não apenas os crimes especificamente previstos na própria lei, mas também qualquer outra infração penal praticada por meios informáticos ou para cuja investigação seja necessária a obtenção de prova em suporte eletrónico. Esta solução amplíssima – que não é mais que o espelho "doméstico" do artigo 14.º, n.º 2, alínea c), da Convenção de Budapeste – é um dos traços mais relevantes do modelo adotado pelo legislador português.

2. O ponto de contacto da Polícia Judiciária (artigos 20.º-21.º LCC)

No que especificamente respeita ao tema do presente artigo, o artigo 20.º da LCC estabelece o dever geral de cooperação internacional, afirmando que as autoridades nacionais cooperam com autoridades estrangeiras para investigações relativas a crimes informáticos e para a recolha de prova eletrónica, em conformidade com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto. O artigo 21.º, n.º 1 densifica este dever, atribuindo à Polícia Judiciária o papel de ponto de contacto nacional em permanência para a rede de cooperação operacional prevista na Convenção de Budapeste.

As competências atribuídas ao ponto de contacto incluem a prestação de aconselhamento técnico a outros pontos de contacto, a preservação expedita de dados em casos de urgência ou perigo na demora, a recolha de prova para a qual seja competente em casos de urgência ou perigo na demora, a localização de suspeitos e a prestação de informações jurídicas em

[4] Aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, e ratificada pelo Decreto do Presidente da República n.º 91/2009, de 15 de setembro (Diário da República, 1.ª Série, n.º 179, 15 de setembro de 2009).

[5] Sobre o âmbito de aplicação do artigo 11.º da Lei do Cibercrime, v. Pedro Verdelho, «A nova Lei do Cibercrime», Scientia Iuridica, Outubro-Dezembro 2009, Tomo LVIII – Número 320, Braga. 2009, pp. 733-735.

contexto de urgência, e a transmissão imediata ao Ministério Público dos pedidos nas situações não urgentes[6]. Esta arquitetura não deixa de ser coerente com a direção do inquérito pelo Ministério Público, postulando, porém, deste último, «*a disponibilidade de magistrados e meios técnicos para levar a cabo quaisquer intervenções processuais urgentes da sua competência*» (artigo 21.º, n.º 4, LCC).

3. Preservação e revelação expeditas de dados informáticos (artigos 22.º-23.º LCC)

O artigo 22.º concretiza no plano doméstico o mecanismo de preservação expedita de dados informáticos previsto nos artigos 16.º e 17.º da Convenção de Budapeste.

A ordem de preservação de dados informáticos armazenados num sistema informático deve identificar, sob pena de nulidade, a natureza dos dados a preservar, a respetiva origem e destino (se conhecidos), e o período de preservação.

O prazo máximo de preservação é de três meses, prorrogável[7].

Destaca-se, nos requisitos formais da solicitação, previstos no n.º 2 do referido artigo 22.º, a necessidade de a solicitação especificar a intenção de a autoridade requisitante apresentar um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação de dados.

O artigo 23.º enumera os motivos de recusa de um pedido de preservação formulado por uma autoridade estrangeira:

- quando os dados a preservar respeitarem a infração de natureza política ou infração conexa segundo as conceções do direito português;
- quando a solicitação atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos; ou
- quando o Estado requisitante não oferecer garantias adequadas de proteção de dados pessoais.

Pode, também, a solicitação ser recusada quanto existirem fundadas razões para crer que a execução do subsequente pedido de auxílio judiciário a formular pela autoridade requisitante para fins de pesquisa, apreensão e divulgação de dados seria recusada, por ausência da verificação do requisito da dupla incriminação (artigo 23.º, n.º 2, LCC).

[6] O artigo 21.º, n.º 4, da Lei do Cibercrime estabelece que o ponto de contacto transmite imediatamente ao Ministério Público todos os pedidos que receba e que respeitem a medidas que carecem de autorização judicial, por não se enquadrarem nos casos de urgência previstos nos números anteriores.
[7] Nos termos da al. c) do n.º 5 do artigo 22.º da Lei do Cibercrime. Porém, nos termos do n.º 7, pode ser renovada a medida por idênticos períodos, até ao limite máximo de um ano.

4. Acesso, acesso transfronteiriço e interseção (artigos 24.º-26.º LCC)

O acesso aos dados informáticos em execução de um pedido de autoridade estrangeira competente é regulado no artigo 24.º, de uma forma simultaneamente ampla e restritiva. Com efeito, aí se estatui que a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos à multiplicidade de crimes previstos no artigo 11.º, mas apenas quando se trate de situação em que a pesquisa e a apreensão seriam admissíveis em caso nacional semelhante.

Já no artigo 25.º é regulado o acesso transfronteiriço a dados armazenados sem ser necessário formular prévio pedido às autoridades nacionais, circunscrevendo-o a dados publicamente disponíveis ou obtidos com consentimento legal e voluntário. Este é um dos raros casos em que a lei reconhece explicitamente que uma autoridade estrangeira possa aceder a dados situados em Portugal sem recurso aos mecanismos formais de cooperação, mas apenas dentro dos estritos limites aí estabelecidos.

Por fim, o artigo 26.º contempla a interseção de comunicações por via de sistema informático localizado em Portugal a pedido de autoridade estrangeira competente, exigindo a intervenção em cadeia da Polícia Judiciária, do Ministério Público e do Juiz de Instrução Criminal da comarca de Lisboa.

III. A CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME

1. Alcance e natureza

Adotada no âmbito do Conselho da Europa em 23 de novembro de 2001[8], a Convenção Sobre o Cibercrime, comummente denominada "Convenção de Budapeste" é considerada o instrumento jurídico internacional de referência em matéria de cibercriminalidade. A sua singularidade decorre de um conjunto de fatores.

Com efeito, tendo sido o primeiro tratado multilateral nesta matéria, veio estabelecer um vocabulário técnico-jurídico comum, erigir tipos de crime harmonizados, criar mecanismos processuais específicos para a obtenção de prova digital, e veio a assumir uma vocação universal, progressivamente adotada por países de todos os continentes[9].

[8] Convenção sobre o Cibercrime (referência do Conselho da Europa STE n.º 185), aberta à assinatura em Budapeste em 23 de novembro de 2001, em vigor desde 1 de julho de 2004. O número de Estados-Parte tem vindo a aumentar, incluindo países que não são membros do Conselho da Europa, através do procedimento de convite previsto no artigo 37.º da Convenção.

[9] Segundo a última atualização disponível, à data da apresentação em que este artigo se baseia (abril de 2026), eram 81 os Estados-Parte da Convenção de Budapeste, o que demonstra a sua consolidação enquanto instrumento de referência global na luta contra a cibercriminalidade.

O Comité da Convenção sobre o Cibercrime (T-CY)[10], instituído no seu artigo 46.º, funciona como uma plataforma de avaliação, interpretação e implementação, emitindo notas de orientação (*guidance notes*) que, não sendo vinculativas, adquiriram considerável autoridade interpretativa.

2. Medidas processuais

Na Secção 2 do seu Capítulo II (medidas a adotar a nível nacional) a Convenção estabelece um conjunto de medidas processuais que os Estados Parte se comprometeram a adotar no seu direito interno.

O artigo 14.º define o âmbito – alargado – de aplicação, que inclui não apenas os crimes tipificados nas "disposições penais materiais", mas também qualquer crime cometido através de um sistema informático ou para cuja investigação seja necessária prova eletrónica.

Os mecanismos mais relevantes para a cooperação internacional são:

- a conservação expedita de dados informáticos armazenados (artigo 16.º, correspondente ao artigo 12.º da Lei do Cibercrime);
- a conservação expedita e divulgação parcial de dados de tráfego (artigo 17.º, correspondente ao artigo 13.º da LCC);
- a injunção para apresentação ou concessão de acesso a dados (artigo 18.º, correspondente ao artigo 14.º da LCC);
- a busca e apreensão de dados informáticos (artigo 19.º, correspondente aos artigos 15.º a 17.º da LCC);
- e a recolha, em tempo real, de dados de tráfego e de conteúdo (artigos 20.º-21.º, correspondentes ao artigo 18.º da LCC).

3. Mecanismos de cooperação internacional

O Capítulo III da Convenção é dedicado à cooperação internacional.

Os artigos 23.º a 28.º estabelecem os princípios gerais que regem a cooperação entre os Estados Parte.

O artigo 23.º afirma o princípio da cooperação mais ampla possível (widest possible *cooperation*), impondo que os Estados se prestem mutuamente auxílio para fins de investigação e procedimento penal relativos a infrações relacionadas com sistemas e dados informáticos, bem como para a recolha de provas em formato eletrónico de qualquer infração penal. Esta

[10] O T-CY foi instituído pelo artigo 46.º da Convenção de Budapeste como órgão colegial de acompanhamento e plataforma de interpretação e implementação da Convenção. As notas de orientação (*guidance notes*) emitidas pelo T-CY, embora não vinculativas, têm influenciado significativamente a interpretação das disposições convencionais pelas autoridades judiciárias nacionais.

cláusula geral de cooperação é estruturante: ativa-se mesmo quando não existe um instrumento convencional específico aplicável ao caso concreto.

O artigo 24.º regula a extradição de pessoas acusadas ou condenadas pelos crimes previstos na Convenção, utilizando a própria Convenção como base jurídica bilateral entre Estados Parte quando não exista tratado de extradição em vigor entre eles.

O artigo 25.º contém princípios gerais sobre auxílio judiciário mútuo, incluindo a possibilidade de recurso a meios técnicos expeditos de comunicação para a prática de atos processuais, e o artigo 27.º admite a tramitação direta de pedidos de auxílio entre autoridades competentes, sem necessidade de envolvimento do canal diplomático, em condições de reciprocidade.

Particularmente relevante é o artigo 28.º, que estabelece o regime de confidencialidade e de limitação de uso das informações e provas transmitidas ao abrigo da Convenção.

A autoridade requerida pode, porém, condicionar a transmissão à aceitação, pelo Estado requerente, de limitações ao uso dos dados – princípio da especialidade em sentido alargado – e pode exigir que os dados recebidos sejam tratados com o mesmo nível de confidencialidade exigido no Estado de origem.

Nos meios específicos de auxílio judiciário mútuo, avulta desde logo a conservação expedita de dados informáticos armazenados, prevista no artigo 29.º, que é a transposição para o plano internacional do mecanismo de conservação expedita previsto nos artigos 16.º e 17.º da Convenção na sua dimensão bilateral.

Quando uma autoridade de um Estado Parte necessita que dados armazenados no território de outro Estado Parte sejam preservados enquanto um pedido formal de auxílio judiciário é preparado e transmitido, pode solicitar diretamente que o Estado requerido ordene a conservação imediata desses dados junto do respetivo prestador de serviços.

O prazo de conservação mínimo garantido é de sessenta dias, renovável.

Trata-se de um mecanismo de urgência que não configura uma produção de prova: os dados ficam preservados enquanto o pedido formal de auxílio é tramitado pelos canais formais, impedindo a sua eliminação durante esse período.

Mas para além da mera conservação, o artigo 30.º regula a divulgação expedita de dados de tráfego permitindo que, numa cadeia de comunicações multijurisdicional, o Estado requerido transmita ao Estado requerente os dados de tráfego suficientes para identificar os prestadores de serviços e a rota das comunicações, mesmo que a produção completa dos dados exija um pedido formal subsequente. Esta disposição é especialmente útil em investigações que envolvam ataques informáticos com múltiplas camadas de anonimização, onde o rastreio da comunicação exige a identificação sequencial de vários prestadores em diferentes jurisdições.

Enquanto os artigos 29.º e 30.º consagram medidas cautelares, o artigo 31.º cria um mecanismo específico de auxílio judiciário mútuo para o acesso a dados informáticos

armazenados no território do Estado requerido. Um pedido ao abrigo desta disposição pode solicitar a pesquisa ou apreensão de dados, bem como a sua conservação e transmissão.

O artigo 31.º é, na prática, a principal via para a obtenção de dados de conteúdo entre Estados Parte, pelo menos enquanto o Segundo Protocolo Adicional não estiver em vigor.

O artigo 32.º é uma das disposições mais arrojadas da Convenção, pois consagra dois casos em que uma autoridade pode aceder diretamente a dados informáticos situados noutro Estado Parte sem necessidade de pedido de auxílio. Tal pode suceder quando os dados são publicamente disponíveis (*open source*), independentemente da sua localização ou quando a autoridade obtém o consentimento legal e voluntário da pessoa que tem autoridade legal para os divulgar.

Esta última hipótese assume alguma controvérsia, tendo-se colocado a questão de saber quem possui legitimidade para consentir na divulgação de dados armazenados num servidor situado noutro país, designadamente, se o titular da conta ou o próprio prestador de serviços em cujo servidor estiverem armazenados os dados. O T-CY debruçou-se sobre esta matéria[11], – de uma forma que podemos apodar de muito cautelosa – remetendo em última instância para as normas domésticas aplicáveis, sem todavia deixar de notar que, em princípio, não seria a entidade meramente custodiante dos dados que teria legitimidade para deles, por assim dizer, dispor.

A negociação do Segundo Protocolo Adicional não ampliou o artigo 32.º(b), mas respondeu ao problema por uma via diferente, criando, no seu artigo 7.º, um mecanismo de ordens diretas de autoridades nacionais a prestadores de serviços situados noutro Estado Parte, baseadas em mandado judicial e não em consentimento, suprindo assim a insuficiência do regime da Convenção original para o acesso transfronteiriço a dados de assinante.

Uma inovação assinalável foi instituída no artigo 35.º da Convenção – a rede permanente de pontos de contacto entre os Estados Parte, disponível vinte e quatro horas por dia, sete dias por semana.

As funções desta rede vão além da mera transmissão de pedidos, incluindo a prestação de aconselhamento técnico e jurídico, a assistência na preservação expedita de dados e a facilitação da comunicação em tempo real entre autoridades.

---

[11] O T-CY adotou, em dezembro de 2014, *a Guidance Note #3 on Transborder Access to Data (Article 32)*, clarificando que o artigo 32.º, al. b), apenas cobre o acesso com consentimento da pessoa que tem autoridade legal para divulgar os dados em relação ao sistema informático em causa, e que seria impróprio considerar que os prestadores de serviços teriam legitimidade para validamente consentir na divulgação de dados de que são meros detentores. «*Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent. Of course, law enforcement agencies may be able to procure data transnationally by other methods, such as mutual legal assistance or procedures for emergency situations*» V. Conselho da Europa, T-CY(2014)25, de 3 de dezembro de 2014: (https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf).

Em Portugal, o ponto de contacto está atualmente sediado na Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) da Polícia Judiciária, que integra simultaneamente a rede da Interpol e o sistema de pontos de contacto da União Europeia no âmbito da Europol[12].

A rede 24/7 é particularmente relevante na prática operacional. Em casos de urgência – por exemplo, ataques de *ransomware*, distribuição de conteúdo de abuso sexual infantil em tempo real, ou comprometimento de infraestruturas críticas – a comunicação direta entre pontos de contacto permite desencadear pedidos de preservação de dados em prazos incompatíveis com a tramitação formal dos canais diplomáticos ou do auxílio judiciário tradicional.

O ponto de contacto recetor pode ainda fazer a ligação entre a autoridade estrangeira e o prestador de serviços relevante no seu território, facilitando a identificação do interlocutor correto num ecossistema de múltiplos prestadores.

IV. O SEGUNDO PROTOCOLO ADICIONAL À CONVENÇÃO DE BUDAPESTE

1. Contexto e objetivos

O Segundo Protocolo Adicional à Convenção sobre o Cibercrime[13], adotado em novembro de 2021 e aberto à assinatura em maio de 2022, pretende responder a uma dupla lacuna que a prática da cooperação internacional veio a identificar: a morosidade e inadequação dos mecanismos formais de auxílio judiciário mútuo perante o volume e a urgência dos pedidos de prova eletrónica e a ausência de instrumentos que permitam às autoridades obter diretamente dos prestadores de serviços dados de assinante e informações de registo de domínios, sem necessidade de recorrer aos canais formais de auxílio judiciário mútuo.

O Protocolo cria mecanismos de cooperação direta com prestadores de serviços (artigos 6.º e 7.º – registo de domínios e dados de assinante) e com serviços de registo, mas também mecanismos de reforço de cooperação entre autoridades mais expeditos para dados de tráfego (artigo 8.º) e para situações de emergência (artigos 9.º e 10.º).

---

[12] A UNC3T integra ainda a rede ECTEG (European Cybercrime Training and Education Group) e coopera com o EC3 (European Cybercrime Centre) da Europol.

[13] O Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e à divulgação de provas eletrónicas (STE n.º 224) foi adotado pelo Comité de Ministros do Conselho da Europa em 17 de novembro de 2021 e aberto à assinatura em 12 de maio de 2022, no âmbito de uma conferência internacional realizada em Estrasburgo. Portugal assinou-o nessa data, integrando o grupo dos 22 Estados que apuseram a sua assinatura na cerimónia de abertura (V. Conselho da Europa, Treaty Office, Chart of Signatures and Ratifications of Treaty 224, disponível em: https://www.coe.int/en/web/conventions/full- list?module=signatures-by-treaty&treatynum=224).
A assinatura pelos Estados-Membros da UE foi autorizada por decisão do Conselho da UE, adotada na sequência da autorização da Comissão para participar nas negociações concedida em 6 de junho de 2019, e a ratificação pelos Estados-Membros foi autorizada pela Decisão do Conselho (UE) 2023/436, de 14 de fevereiro de 2023, JO L 63, 28 de fevereiro de 2023, pp. 48-53.

O Segundo Protocolo complementa – sem substituir – os mecanismos da Convenção, estabelecendo canais de cooperação mais ágeis para situações específicas.

Nos termos do seu artigo 16.º, n.º 3, a sua entrada em vigor exige cinco ratificações. À data de elaboração deste artigo, 52 países haviam assinado o Segundo Protocolo e, desses, 4 completado o processo de ratificação[14]. Portugal, que assinou o Protocolo na data de abertura à assinatura, ainda não o ratificou.

2. Cooperação direta com entidades privadas (artigos 6.º-7.º)

A inovação mais significativa do Segundo Protocolo consiste, pois, na criação de um mecanismo de cooperação direta entre uma autoridade de um Estado Parte e entidades privadas – nomeadamente prestadores de serviços de registo de domínios (artigo 6.º) e prestadores de serviços de internet no que respeita a dados de assinantes (artigo 7.º) – sediadas noutro Estado Parte, sem necessidade de intervenção das autoridades do país em que se encontrem domiciliadas[15].

Com efeito, estabelece o artigo 6.º a possibilidade de as autoridades competentes de um Estado Parte apresentarem diretamente a uma entidade que preste serviços de registo de nomes de domínio no território de outro Estado Parte, um pedido de informações com vista a identificar ou contactar o titular registado de um nome de domínio.

Já o artigo 7.º prevê que as autoridades competentes de um Estado Parte possam emitir uma injunção a apresentar diretamente a um prestador de serviços localizado no território de outro Estado Parte, ordenando-lhe que comunique dados específicos armazenados relativos aos assinantes. Nos termos do n.º 7 deste artigo, o prestador de serviços tem a faculdade de recusar, devendo nesse caso justificar a recusa. Em caso de recusa e em caso de não resposta à injunção no prazo de trinta dias, pode ser acionado o mecanismo de execução previsto no artigo 8.º.

3. Execução expedita de injunções (artigo 8.º)

O artigo 8.º cria um mecanismo simplificado de cooperação interestadual para situações em que uma autoridade de um Estado Parte pretende que a autoridade de outro Estado Parte execute uma injunção dirigida a um prestador fisicamente presente no seu território. Este mecanismo é mais expedito do que o auxílio judiciário mútuo tradicional, com prazos de resposta de vinte dias para dados de assinantes e quarenta e cinco dias para dados de tráfego.

---

[14] Até à data de elaboração do presente artigo (junho de 2026), Sérvia, Japão, Hungria e Costa Rica ratificaram o Segundo Protocolo Adicional, sendo o último a Costa Rica, em abril de 2026: (https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224).

[15] Sobre as limitações do mecanismo de cooperação direta com entidades privadas previsto nos artigos 6.º e 7.º do Segundo Protocolo, mas assinalando a vocação universal do Segundo Protocolo (nessa medida beneficiando, comparativamente ao pacote legislativo comunitário, da vocação universalista da Convenção de Budapeste), v. Stanisław Tosza, «Electronic Evidence after the E-Evidence Package's Adoption: Challenges for Application and Unresolved Problems», Studia Iuridica Lublinensia, vol. 33, 5, 2024.

4. Comunicação expedita em emergência (artigo 9.º) e proteção de dados

O artigo 9.º prevê a possibilidade de, em casos de emergência – como sejam ataques terroristas, ataques de *ransomware* a sistemas críticos, p. ex. instalações hospitalares ou transportes, ou investigações de sequestro com comunicação em curso –, uma autoridade solicitar a uma sua congénere a transmissão urgente de dados armazenados por prestadores de serviços no seu território, utilizando o canal da rede 24/7, sem necessidade de pedido formal de auxílio mútuo.

O Capítulo III do Segundo Protocolo, dedicado à proteção de dados, estabelece salvaguardas relevantes, nos artigos 13.º e 14.º, estabelecendo, nomeadamente, que os dados partilhados ao abrigo do Protocolo apenas podem ser utilizados para os fins para que foram transmitidos, que a partilha com países terceiros ou organizações internacionais requer autorização prévia do Estado transmitente e que os titulares dos dados têm direito a reclamação junto de autoridades de supervisão.

V. O PACOTE LEGISLATIVO EUROPEU E-EVIDENCE

1. Contexto

O pacote legislativo europeu sobre prova eletrónica – composto pelo Regulamento (UE) 2023/1543[16] (Regulamento) e pela Diretiva (UE) 2023/1544[17] (Diretiva) – representa a resposta da União Europeia à inadequação dos instrumentos de cooperação judiciária relativamente às especificidades da prova eletrónica[18].

A proposta da Comissão, apresentada em abril de 2018, foi alvo de um prolongado processo legislativo que, após intensas negociações, culminou na adoção formal em julho de 2023.

O Regulamento vem instituir as Ordens Europeias de Produção (OEP) e Ordens Europeias de Conservação (OEC) para efeitos de obtenção de prova electrónica em processos penais e para efeitos de execução de penas privativas da liberdade na sequência de processos penais e será aplicável a partir de 18 de agosto de 2026[19].

---

[16] Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e de conservação de provas eletrónicas em processo penal e para efeitos da execução de sanções penais, JO L 191, de 28 de julho de 2023, pp. 1-39.

[17] Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, que estabelece regras harmonizadas relativas à designação de estabelecimentos ou à nomeação de representantes legais para efeitos da recolha de provas em processos penais, JO L 191, de 28 de julho de 2023, pp. 40-49.

[18] A avaliação de impacto que acompanhou a proposta legislativa da Comissão Europeia (SWD(2018) 118 final) concluiu que os instrumentos existentes, nomeadamente a Decisão-Quadro 2002/465/JAI sobre equipas de investigação conjunta, a Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal de 1959 e a Diretiva 2014/41/UE sobre a Decisão Europeia de Investigação, não se adequavam às especificidades da prova eletrónica.

[19] Nos termos do artigo 34.º, n.º 2, do Regulamento, este é aplicável a partir de 18 de agosto de 2026, exceto para a Dinamarca que exerceu o seu direito de não participação (*opt-out*) em matéria de cooperação judiciária penal.

Quanto à Diretiva, vem estabelecer regras harmonizadas aplicáveis à designação de estabelecimentos e à nomeação de representantes legais, para efeitos de recolha de prova electrónica em processos penais. Visa, pois, harmonizar as regras que cada Estado terá de adotar tendentes à designação dos destinatários das OEP e OEC.

2. Âmbito de aplicação subjetivo do Regulamento (artigo 2.º)

Nos termos do artigo 2.º, n.º 1, o Regulamento «*é aplicável aos prestadores de serviços que ofereçam serviços na União*».

De um ponto de vista subjetivo, o Regulamento dirige-se a todos os prestadores de serviços que ofereçam os seus serviços na União Europeia[20], independentemente da sua sede ou da localização física dos dados.

O critério determinante é, portanto, o mercado servido e não o estabelecimento.

Para efeitos do Regulamento são abrangidos, grosso modo, três grupos de prestadores: os que asseguram comunicações eletrónicas (incluindo serviços de voz sobre IP, mensagens instantâneas e correio eletrónico); os que gerem infraestruturas de identificação e endereçamento na rede, como os serviços de registo de domínios, atribuição de endereços IP e proxy; e os que prestam outros serviços da sociedade da informação que impliquem comunicação ou armazenamento de dados por conta dos utilizadores (categoria que abrange plataformas de redes sociais, serviços de computação em nuvem, mercados digitais e serviços de alojamento).

Esta delimitação material é assim simultaneamente ampla, abrangendo os serviços que, na prática, detêm a grande maioria da prova digital relevante para as investigações criminais, e funcional, na medida em que o critério decisivo não é a natureza jurídica do prestador nem a sua localização, mas sim o facto de oferecer serviços na União Europeia. Um prestador sediado nos Estados Unidos que ofereça uma plataforma de redes sociais a utilizadores portugueses está, portanto, abrangido pelo Regulamento.

3. Âmbito de aplicação objetivo (artigos 2.º e 3.º do Regulamento)

O Regulamento tem, desde logo, uma limitação objetiva importante, uma vez que abrange exclusivamente dados já armazenados no momento em que a ordem é recebida, não se aplicando à interceção de comunicações em tempo real.

A distinção entre dados históricos armazenados e dados em circulação permanece, assim, juridicamente operativa, e os mecanismos de interceção de dados em tempo real continuam a reger-se pelas normas nacionais e pelos instrumentos de cooperação tradicionais.

[20] Sobre a tipologia dos prestadores de serviços abrangidos e as respetivas obrigações, v. considerandos 26 a 30 do Regulamento (UE) 2023/1543.

A distinção entre as categorias de dados é um dos eixos estruturantes deste Regulamento, pois determina simultaneamente o limiar de infração penal exigido para a emissão da ordem, a(s) autoridade(s) competente(s) para a emitir, a obrigatoriedade ou não de notificação ao Estado de execução, e os fundamentos de recusa disponíveis. O Regulamento distingue quatro categorias de dados:

- Os dados de assinante (*subscriber data*) englobam os elementos de identificação civil e contratual que o prestador detém sobre o utilizador: informações de contacto, dados de faturação e dados relativos ao tipo e duração do serviço contratado[21]. Tratando-se da categoria com menor potencial de intrusão na privacidade – identificam quem é o utilizador, mas não o que faz – o Regulamento sujeita-a ao regime menos exigente: uma OEP de dados de assinante pode ser emitida para investigar qualquer infração penal para a qual a pena máxima prevista não seja inferior a quatro meses de prisão[22], e a sua emissão é admissível por magistrado do Ministério Público ou por autoridades de investigação competentes, não estritamente judiciais (aqui com eventual validação)[23], sem obrigação de notificação ao Estado de execução[24];

- Os dados solicitados para identificação do utilizador (*access data)* constituem uma subcategoria dos dados de assinante especificamente delimitada: referem-se aos endereços IP, às marcas temporais (*timestamps*) e aos números de porta utilizados numa determinada sessão, exclusivamente na medida necessária para identificar o utilizador[25]. A sua especificidade – são o instrumento essencial para percorrer o trajeto entre um endereço IP e a identidade de uma pessoa – justificou a sua autonomização. Nesse sentido, quando solicitados exclusivamente para identificação, partilham o regime dos dados de assinante, mas quando utilizados para fins mais amplos, como estabelecer o perfil de comunicações do utilizador, são tratados como dados de tráfego, sujeitos ao regime mais exigente[26].

- Os dados de tráfego (*traffic data*) abrangem todos os dados eletrónicos gerados ou tratados no âmbito de uma comunicação que permitam identificar a sua origem, o destino, o trajeto, a data, a hora, a duração, o tamanho e o tipo de serviço

[21] Nos termos do artigo 3.º, n.º 9, do Regulamento (UE) 2023/1543, os «dados de assinantes» incluem: o nome, a data de nascimento, o endereço postal, o número de telefone, o endereço de correio eletrónico e o endereço IP no momento do registo, o tipo de serviço contratado e os dados de faturação, bem como – quando relevante – o número de identificação do dispositivo utilizado.
[22] Artigo 5.º, n.º 3, do Regulamento.
[23] Artigo 4.º, n.º 1, do Regulamento.
[24] Artigo 8.º, n.º 1, *a contrario* do Regulamento.
[25] O conceito de «*dados solicitados com o único objetivo de identificar o utilizador*» (access data), previstos no artigo 3.º, n.º 10, foi introduzido pelo legislador europeu para preencher um espaço que na Convenção de Budapeste era tratado de forma ambígua, ora como dados de tráfego, ora como dados de assinante. A sua autonomização permite sujeitar pedidos de identificação de titular de endereço IP ao regime menos exigente dos dados de assinante, sem alargar indevidamente essa solução a todo o espectro dos metadados das comunicações. Sobre a génese da distinção, v. Tosza, cit. na nota 15.
[26] V. considerandos 32 e 33 do Regulamento.

subjacente, sem revelar o seu conteúdo[27].

Incluem, designadamente, os registos de chamadas, os metadados de correio eletrónico (destinatários, datas, assuntos), os registos de sessão em plataformas digitais e os dados de localização associados às comunicações.

São dados com uma sensibilidade intermédia: revelam padrões de comportamento e de relacionamento sem expor o conteúdo das comunicações, mas permitem reconstituir o trajeto de uma comunicação com um nível de detalhe que não é negligenciável.

Por essa razão, a obtenção de dados de tráfego está sujeita a um limiar de gravidade penal mais elevado.

O Regulamento exige, para a emissão de uma OEP de dados de tráfego, que a infração seja punível com pena privativa de liberdade de duração máxima não inferior a três anos, ou que se enquadre no catálogo de crimes do art. 5.º, n.º 4, alíneas. b) e c)[28] mesmo que a pena prevista não atinja aquele limiar.

A competência emissora é exclusivamente judicial ou com validação obrigatória por juiz – exceto em emergência devidamente justificada[29]– e a notificação ao Estado de execução é obrigatória, salvo quando há ligação substancial ao Estado de emissão[30];

- Os dados de conteúdo (*content data*) são, por definição, o substrato semântico das comunicações e dos ficheiros armazenados digitalmente: tudo aquilo que o utilizador escreveu, disse, filmou, partilhou ou guardou[31]. O legislador europeu optou por uma definição parcialmente residual, o que lhe confere uma amplitude considerável. São a categoria mais sensível sob o ponto de vista dos direitos fundamentais e aquela para a qual o Regulamento estabelece o regime mais exigente: os limiares de gravidade penal são os mesmos que para os dados de tráfego[32]; a competência emissora é exclusivamente judicial, com validação obrigatória por juiz ou tribunal[33]; a notificação ao Estado de execução é sempre obrigatória, com efeito suspensivo sobre as obrigações de entrega pelo prestador[34]; e a autoridade emissora não pode emitir a OEP se concluir que os dados estão protegidos por imunidades, privilégios ou regras sobre liberdade de imprensa ao

[27] A definição de dados de tráfego no Regulamento (UE) 2023/1543 (artigo 3.º, n.º 11) é mais ampla que a da Convenção de Budapeste (artigo 1.º, al. d)), na medida em que abrange expressamente os dados de localização gerados no contexto das comunicações.

[28] Que abrange as infrações informáticas (Diretiva 2013/40/UE), o terrorismo (Diretiva 2017/541), as infrações contra crianças (Diretiva 2011/93/UE) e a fraude e falsificação de meios de pagamento (Diretiva 2019/713).

[29] Artigo 4.º, n.º 2, do Regulamento.

[30] Artigo 8.º, n.ºs 1 e 2, do Regulamento.

[31] O legislador europeu optou por uma definição residual de «*dados de conteúdo*» no Regulamento (UE) 2023/1543 (artigo 3.º, n.º 11): pertencem a esta categoria todos os dados armazenados digitalmente que não sejam qualificáveis como dados de assinante, de identificação do utilizador ou de tráfego, abrangendo portanto qualquer representação digital com valor semântico – texto, voz, imagens, vídeo ou som – que o utilizador tenha criado ou armazenado.

[32] Artigo 5.º, n.º 4, do Regulamento.

[33] Artigo 4.º, n.º 2, do Regulamento.

[34] Artigo 8.º, n.ºs 1 e 4 do Regulamento.

abrigo do direito do Estado de execução[35]. O Regulamento estabelece ainda que dados de tráfego e de conteúdo que beneficiem dessas proteções não podem ser objeto de OEP, independentemente de qualquer outra consideração.

4. Condições materiais de emissão e princípios transversais (artigo 5.º)

O artigo 5.º estabelece as condições materiais de emissão aplicáveis às OEP e OEC, que funcionam como garantias de fundo, independentes das condições processuais de cada tipo de ordem. São consagrados princípios com um alcance transversal.

Os princípios da necessidade e proporcionalidade impõem que qualquer ordem só possa ser emitida quando for necessária e proporcionada face à finalidade do processo penal em causa, tomando em consideração os direitos do suspeito ou arguido. A autoridade emissora deve, portanto, fundamentar não apenas a relevância dos dados para a investigação, mas também a adequação da medida em face de alternativas menos intrusivas, e a proporcionalidade entre os dados solicitados e a gravidade da infração investigada[36].

O princípio da equivalência com a medida interna é igualmente estruturante: uma OEP ou OEC só pode ser emitida se uma medida equivalente for admissível num caso interno análogo no Estado de emissão. Esta exigência cumpre uma dupla função: impede o *forum shopping* probatório, traduzido na eventual utilização do Regulamento para obter provas que o direito interno não autorizaria, e ancora o novo regime no direito processual de cada Estado, preservando as garantias constitucionais e processuais da ordem jurídica de emissão. Uma autoridade portuguesa não pode emitir uma OEP para obter dados de conteúdo num caso em que a lei portuguesa não admitiria a interceção ou a apreensão de comunicações equivalentes[37].

---

[35] Artigo 5.º, n.º 10, segundo parágrafo.

[36] O princípio da proporcionalidade (em sentido lato) é expressamente mencionado no considerando 38 do Regulamento: «*Uma ordem europeia de produção só deverá ser emitida se for necessária, proporcionada, adequada e aplicável ao processo em apreço. A autoridade emissora deverá ter em conta os direitos do suspeito ou do arguido em processos relacionados com uma infração penal e só deverá emitir uma ordem europeia de produção se essa ordem puder ter sido emitida nas mesmas condições num processo nacional semelhante. A avaliação da emissão de uma ordem europeia de produção deverá ter em conta se a ordem se limita ao estritamente necessário para atingir o objetivo legítimo de obter os dados pertinentes e necessários para serem utilizados como elementos de prova num processo concreto.*».

[37] A condição de equivalência com a medida interna, prevista no artigo 5.º, n.º 2 *in fine* do Regulamento, é um dos mecanismos anti-abuso mais debatidos na doutrina. Tosza, cit. na nota 15, identifica a sua função essencial como a de impedir que o Regulamento seja instrumentalizado para contornar garantias processuais que o direito interno do Estado de emissão recusa – o que o autor designa por «forum shopping» probatório europeu. Para um enquadramento comparado dos padrões de admissibilidade e das regras de exclusão de prova obtida com violação de formalidades legais em contexto transfronteiriço, v. Joep Lindeman / Michiel Luchtman / Dave van Toor, «Admissibility of Evidence in EU Cross-Border Criminal Proceedings», capítulo in Admissibility of Evidence in EU Cross-Border Criminal Proceedings (eds. Lindeman / Luchtman / van Toor), 2024, disponível em https://dspace.library.uu.nl/items/9f7e62aa-cb24-43f2-892d-b0d3c3fa04c6, e para a perspetiva processual comparada sobre exclusão de prova, Thomas Weigend, «The Potential to Secure a Fair Trial Through Evidence Exclusion: A German Perspective», in Do Exclusionary Rules Ensure a Fair Trial? (Sabine Gless / Thomas Richter, eds.), Intersentia, 2019, pp. 61-88, disponível também em:

5. Obrigações dos prestadores e fundamentos de não execução (artigos 10.º e seguintes)

As obrigações do prestador variam consoante o tipo de ordem recebida.

A receção de uma OEC obriga à imediata suspensão de qualquer eliminação ou alteração dos dados identificados.

O período inicial de conservação é de sessenta dias, renovável por mais trinta a pedido da autoridade emissora, e converte-se em prazo indeterminado se entretanto for emitida uma OEP. Perante uma OEP, o prestador deve conservar e transmitir os dados no prazo de dez dias (ou de oito horas em casos de emergência)[38], garantindo simultaneamente a confidencialidade da ordem e a integridade dos dados transmitidos[39].

O cumprimento de boa-fé de uma OEC ou de uma OEP isenta o prestador de responsabilidade civil perante os utilizadores ou terceiros pelos prejuízos causados, ressalvadas as obrigações em matéria de proteção de dados. Esta imunidade é essencial para que os prestadores cooperem sem receio de litígios por parte dos titulares dos dados.

O não cumprimento das obrigações do Regulamento sujeita o prestador a sanções pecuniárias cuja previsão e regulamentação é cometida aos Estados-Membros.

O Regulamento estabelece, não obstante, um teto sancionatório calculado em função do volume de negócios global do prestador – fixado em dois por cento da faturação mundial anual, nos termos do artigo 15.º – parâmetro que, aplicado às grandes plataformas tecnológicas, pode atingir montantes da ordem dos milhares de milhões de euros.

A execução coerciva, quando o prestador não cumpra voluntariamente, compete ao Estado de execução, que dispõe de cinco dias úteis para atuar após solicitação da autoridade emissora (artigo 16.º, n.º 2, do Regulamento).

O Regulamento distribui por três regimes distintos as situações em que a execução de uma OEP pode não ter lugar.

O primeiro consiste nos fundamentos de recusa invocáveis pela autoridade de execução, previstos no artigo 12.º, n.º 1 e que serão analisados *infra* em **6.**.

---

https://lgcl.csl.mpg.de/attachments/Weigend_2019_The_potential_to_secure_a_fair_trial_through_evidence_ exclusion.pdf.

[38] Situações de emergência definidas no artigo 3.º, n.º 18 do Regulamento, que incluem a ameaça iminente à vida ou à integridade física de uma pessoa, à segurança pública, ou a infraestruturas críticas.

[39] As obrigações do prestador na execução de uma OEC e de uma OEP estão detalhadas nos artigos 10.º a 14.º do Regulamento (UE) 2023/1543. Merece destaque a obrigação de confidencialidade (artigo 13.º): o prestador não pode, em regra, informar o titular dos dados da existência da ordem, salvo autorização da autoridade emissora. O incumprimento desta obrigação de confidencialidade pode ser, em si mesmo, passível de sanção pecuniária ao abrigo do artigo 15.º, n.º 1, do Regulamento.

O segundo regime é o das situações de incumprimento justificado pelo prestador (artigo 10.º, n.ºs 5, 6 e 7): o prestador não recusa autonomamente, mas informa a autoridade emissora e, quando aplicável, a autoridade de execução. Neste regime cabem três hipóteses:

– a interferência com imunidades ou privilégios que o prestador identifica exclusivamente com base nas informações do certificado de OEP (n.º 5);

– o certificado de OEP estar incompleto, com erros manifestos ou insuficiente para execução, caso em que o prestador solicita clarificação e as obrigações ficam suspensas até à resposta (n.º 6);

– e a impossibilidade de facto por circunstâncias não imputáveis ao prestador (n.º 7)

Nenhum destes casos configura uma recusa definitiva por parte do prestador, ficando este a aguardar clarificação ou dispensa por parte da autoridade emissora.

O terceiro regime é o procedimento de reexame por conflito com a lei de país terceiro (artigo 17.º). Aqui, o prestador notifica o conflito com uma obrigação prevista no direito aplicável de um país terceiro através de um formulário próprio para o efeito, de «*oposição fundamentada*», ficando a execução suspensa enquanto o tribunal competente do Estado de emissão decide confirmar ou revogar a OEP. A decisão final nunca pertence ao prestador[40].

Este último fundamento para não execução – o eventual conflito com legislação de países terceiros – é particularmente relevante para os grandes prestadores estabelecidos fora da União Europeia. A título de exemplo, a legislação dos Estados-Unidos, designadamente o CLOUD Act[41], pode impor ao mesmo prestador obrigações contraditórias com as que decorrem de uma OEP europeia. O artigo 17.º do Regulamento cria para estes casos um procedimento de reexame: o prestador notifica o conflito através de uma oposição

[40] Os fundamentos de não execução pelo prestador estão previstos no artigo 10.º do Regulamento (UE) 2023/1543. O fundamento relativo ao conflito com a legislação de países terceiros foi um dos mais debatidos durante o processo legislativo, tendo originalmente contemplado um mecanismo de revisão judicial pelo Estado de execução que foi significativamente comprimido na versão final. A proposta original da Comissão (COM(2018) 225 final) previa nos artigos 15.º e 16.º um procedimento de revisão judicial pelo Estado de execução para os casos de obrigações conflituantes. Na versão final do Regulamento esse mecanismo foi comprimido para o artigo 12.º, sem procedimento judicial autónomo pelo Estado de execução.
V. https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?qid=1550155986946&uri=CELEX:52018PC0225&from=EN.
Sobre o conflito específico com o CLOUD Act e o acordo bilateral UE-EUA em negociação, v. Tosza, cit. na nota 15. Para o contexto mais amplo das investigações transfronteiriças assentes em grandes volumes de dados digitais, v. Boudewijn de Jonge / Barry de Vries, «Data-Driven Investigations in a Cross-Border Setting», eucrim, Vol. 19(3), 2024, pp. 214-221, DOI: 10.30709/eucrim-2024-020 (artigo centrado nas experiências práticas neerlandesas no âmbito da Diretiva 2016/618, de 27 de abril de 2016, não especificamente sobre o artigo 12.º do Regulamento).

[41] O CLOUD Act (Clarifying Lawful Overseas Use of Data Act) é um ato legislativo adotado pelo Congresso dos Estados Unidos da América a 23 de março de 2018, que habilita os prestadores de serviços locais a partilhar prova eletrónica com autoridades judiciárias e policiais estrangeiras, em processos criminais, desde que exista um acordo bilateral a nível governamental em vigor. Desde a sua adoção, apenas foram celebrados acordosao abrigo desta legislação com o Reino Unido e Austrália, encontrando-se em *stand-by* a realização de acordos com a União Europeia.

fundamentada, apresentada no prazo de 10 dias após a receção da OEP, identificando o direito do país terceiro invocado, a sua aplicabilidade ao caso concreto e a natureza da obrigação em conflito (n.º 2).

A oposição não pode assentar na mera ausência de norma equivalente no país terceiro ou no simples facto de os dados estarem conservados nesse país (n.º 2, als. a) e b)).

A autoridade emissora reexamina a OEP e, se quiser confirmá-la, submete-a ao tribunal competente do Estado-Membro de emissão, ficando a execução suspensa durante esse reexame (n.º 3).

O tribunal competente deve primeiro determinar se existe efetivamente conflito de obrigações – verificando se o direito do país terceiro é aplicável e proíbe a divulgação dos dados nas circunstâncias concretas (n.º 4) – e, se concluir pela existência, decide confirmar ou revogar a OEP com base numa ponderação de fatores que incluem o interesse protegido pelo direito do país terceiro, o grau de ligação do processo penal com cada jurisdição, a gravidade da infração e as possíveis consequências para o prestador (n.º 6).

O tribunal pode ainda solicitar informações à autoridade competente do país terceiro, devendo fazê-lo quando o conflito disser respeito a direitos fundamentais ou a interesses de segurança e defesa nacionais desse país (n.º 7).

6. O papel do Estado de execução (artigos 8.º e 12.º a 16.º)

A notificação ao Estado de execução é obrigatória quando a OEP visa dados de tráfego – com exceção dos solicitados exclusivamente para identificação do utilizador – ou dados de conteúdo (artigo 8.º, n.º 1). Esta obrigação cessa quando a autoridade emissora tiver motivos razoáveis para crer, cumulativamente, que a infração foi cometida ou está a ser cometida no Estado de emissão e que a pessoa cujos dados são solicitados aí reside (artigo 8.º, n.º 2).

A notificação tem efeito suspensivo sobre a obrigação de entrega pelo prestador durante o prazo que a autoridade de execução dispõe para analisar a ordem e eventualmente invocar fundamentos de recusa[42].

Esse prazo é de dez dias em condições normais e de noventa e seis horas em casos de urgência. Durante este período, a autoridade de execução avalia se estão verificados fundamentos de recusa, enunciados taxativamente no artigo 12.º, n.º 1:

- a existência de imunidades ou privilégios ao abrigo da lei do Estado de execução que protejam os dados em causa;

- a existência de motivos substanciais para crer que a execução da ordem constituiria uma violação manifesta dos direitos fundamentais garantidos pela Carta dos Direitos

[42] Nos termos da conjugação do artigo 8.º, n.º 4 e 10.º, n.ºs 2 e 4, a notificação suspende a obrigação de entrega pelo prestador durante 10 dias (96 horas em casos de urgência), período durante o qual a autoridade de execução pode invocar fundamentos de recusa.

Fundamentais da União Europeia;

- a aplicação do princípio *ne bis in idem*, quando a pessoa visada está a ser ou foi julgada no Estado de execução pelo mesmo facto;

- e a ausência de dupla incriminação, para infrações que não constem do Anexo IV do Regulamento e cuja pena máxima seja inferior a três anos.

A autoridade de execução não pode, portanto, invocar razões de oportunidade, de soberania ou de incompatibilidade com o seu sistema processual para recusar a execução de uma OEP. O elenco de fundamentos de recusa é taxativo.

Se a autoridade de execução decidir recusar, deve consultar previamente a autoridade emissora, que dispõe de cinco dias para responder, podendo esta retirar ou adaptar a ordem.

7. Garantias e direitos dos titulares dos dados (artigos 17.º-21.º)

O Regulamento incorpora um conjunto de garantias destinadas a assegurar que o novo sistema de obtenção de prova não prejudica os direitos processuais dos suspeitos, arguidos e titulares de dados.

Em matéria de informação, a autoridade emissora fica obrigada a notificar o titular dos dados da existência da OEP num prazo razoável após a sua emissão – obrigação cujo cumprimento pode, todavia, ser diferido ou restringido quando a revelação prematura ponha em causa o êxito da investigação ou a proteção de terceiros, devendo as razões do diferimento ficar documentadas no certificado OEP.

O direito a vias de recurso efetivas garante aos titulares dos dados o direito de impugnar a legalidade, a necessidade e a proporcionalidade da OEP junto de um tribunal do Estado de emissão, durante o processo penal em que os dados são utilizados.

O suspeito ou arguido, e o seu defensor, podem ainda requerer a emissão de uma OEP ou OEC para fins de defesa, ao abrigo do direito processual nacional, o que representa um reconhecimento inovador da natureza bilateral do sistema.

8. O sistema JUDEX e os desafios de implementação

A transmissão de ordens e comunicações entre autoridades judiciais e prestadores de serviços deverá efetuar-se, quando o sistema estiver operacional, exclusivamente através do sistema informático descentralizado JUDEX.

A utilização do JUDEX será obrigatória e o sistema foi concebido para assegurar comunicações seguras, autenticadas e com rastreabilidade completa.

O artigo 25.º, n.º 3 do Regulamento impunha à Comissão a adoção dos atos de execução necessários até 18 de agosto de 2025, prazo esse que foi cumprido: o Regulamento de

Execução (UE) 2025/1550 da Comissão, de 28 de julho de 2025[43], estabeleceu as especificações técnicas e demais requisitos do sistema.

A obrigação de utilizar o JUDEX torna-se efetiva um ano após essa adoção, praticamente coincidindo com a data de aplicação do Regulamento em agosto de 2026.

Além da questão da disponibilidade do JUDEX, o referido Regulamento de Execução introduz um limite técnico relevante: a prova eletrónica só pode ser transmitida através do sistema descentralizado se não exceder 25 megabytes (25.600 kilobytes), devendo, acima desse limiar, a transmissão efetuar-se por meio alternativo que assegure troca de informação rápida, segura e fiável e permita ao destinatário estabelecer a autenticidade, nos termos do artigo 19.º, n.º 5, do Regulamento. O que se poderá revelar problemático em pedidos envolvendo grandes volumes de dados ou ficheiros multimédia.

À data da elaboração deste artigo, subsistem diversas dúvidas quanto à implementação prática e operacional do sistema pelos Estados-Membros e pelos prestadores.

9. A Diretiva (UE) 2023/1544: representantes legais e estabelecimentos designados

A Diretiva tem uma função instrumental neste sistema, uma vez que não cria quaisquer mecanismos autónomos de obtenção de prova, visando "apenas" assegurar que todos os prestadores que ofereçam serviços na União disponibilizem um ponto de contacto juridicamente responsável – um estabelecimento designado, para os prestadores sediados na UE, ou um representante legal, para os prestadores de fora da União.

A distinção é relevante, pois o estabelecimento designado é uma entidade que integra a estrutura organizacional do próprio prestador e por ela responde, ao passo que o representante legal é uma pessoa singular ou coletiva nomeada para o efeito, que supre a ausência de estabelecimento na União. Seja como for, em ambos os casos, o destinatário está juridicamente obrigado a receber as ordens, a garantir o seu cumprimento e a responder perante as autoridades competentes.

O prazo de transposição da Diretiva expirou em 18 de fevereiro de 2026 sem que Portugal tivesse concluído o processo legislativo[44].

---

[43] Regulamento de Execução (UE) 2025/1550 da Comissão, de 28 de julho de 2025, que estabelece as especificações técnicas e outros requisitos para o sistema informático descentralizado referido no Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho *in* https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32025R1550.

[44] O prazo de transposição da Diretiva (UE) 2023/1544 expirou em 18 de fevereiro de 2026. A Proposta de Lei n.º 83/XVII/1.ª foi aprovada em Conselho de Ministros de 21 de maio de 2026 e admitida na Assembleia da República em 2 de junho de 2026, com pedido de prioridade e urgência. À data de conclusão do presente artigo, a proposta encontrava-se em fase de consulta pública, aguardando apreciação parlamentar. A apresentação extemporânea – com atraso de mais de três meses sobre o prazo de transposição – não exonera o Estado português da responsabilidade perante a Comissão Europeia, mas a aprovação da proposta antes de 18 de agosto de 2026 permitirá ainda evitar a situação mais grave de aplicação plena do Regulamento sem quadro sancionatório interno nem autoridades designadas. A proposta foi apresentada com pedido de prioridade e urgência precisamente para viabilizar a aprovação dentro desse prazo.

10. Referência à Proposta de Lei n.º 83/XVII/1.ª

Aprovada em Conselho de Ministros de 21 de maio de 2026 e apresentada à Assembleia da República em 2 de junho de 2026, a Proposta de Lei n.º 83/XVII/1.ª transpõe a Diretiva (UE) 2023/1544 e estabelece o regime sancionatório aplicável às infrações das normas constantes da mesma Diretiva e do Regulamento (UE) 2023/1543[45].

À data de conclusão do presente artigo, a proposta encontrava-se em fase de consulta pública e apreciação parlamentar.

De um ponto de vista substantivo, a proposta prossegue dois objetivos declarados e outros dois não declarados, mas interligados.

O primeiro é a transposição da Diretiva (UE) 2023/1544, fixando as regras aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais dos prestadores de serviços, definidos como tal no artigo 3.º, alínea c)[46].

Nos termos dos artigos 5.º a 9.º da Proposta, os prestadores de serviços estabelecidos em Portugal e que ofereçam serviços na União Europeia ficam obrigados a designar por escrito pelo menos um estabelecimento designado, enquanto que os prestadores de serviços não estabelecidos na União Europeia mas que ofereçam serviços em Portugal ficam obrigados a nomear um representante legal.

A responsabilidade pela execução das OEP e OEC é solidária entre o prestador de serviços e o respetivo estabelecimento ou representante (artigo 8.º), não podendo a ausência de procedimentos internos adequados ser invocada como justificação para o incumprimento dessas ordens.

Quanto à autoridade central designada para a recolha, organização e tratamento da informação relativa aos estabelecimentos designados e representantes legais será, nos termos do artigo 4.º da Proposta, a Autoridade Nacional de Comunicações (ANACOM), cabendo aos prestadores comunicar os contactos do estabelecimento designado ou do representante legal nomeado à ANACOM e às autoridades centrais dos Estados-Membros onde os estabelecimentos estejam sediados (artigo 9.º).

---

[45] V. https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=356842.

[46] Artigo 3.º da Proposta: «c) «*Prestador de serviços», qualquer pessoa singular ou coletiva que, com exceção dos serviços financeiros, preste uma ou mais das seguintes categorias de serviços:*

i) Serviços de comunicações eletrónicas, tal como se encontram definidos na alínea ss) do n.º 1 do artigo 3.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual;

ii) Serviços de nomes de domínio de Internet e de numeração IP, tais como atribuição de endereços IP, registo de nomes de domínio, agente de registo de nomes de domínio e serviços de privacidade e de proxy relacionados com nomes de domínio;

iii) Outros serviços da sociedade da informação a que se refere a alínea g) do artigo 3.º do Decreto-Lei n.º 30/2020, de 29 de junho, que permitam aos seus utilizadores comunicarem entre si ou que possibilitem a conservação ou outro tipo de tratamento de dados em nome dos utilizadores a quem o serviço é prestado, sempre que a conservação de dados seja uma componente determinante do serviço prestado ao utilizador;».

Os prestadores que em 18 de fevereiro de 2026 ofereçam serviços na União Europeia dispõem até 18 de agosto de 2026 para cumprir esta obrigação (artigo 22.º).

O segundo objetivo declarado da Proposta é o estabelecimento do regime sancionatório exigido pelo artigo 15.º, n.º 1, do Regulamento (UE) 2023/1543.

Nos artigos 10.º a 18.º, a Proposta estabelece dois graus de contraordenações.

Constituem contraordenações muito graves (artigo 10.º, n.º 1) a falta de designação de estabelecimento ou nomeação de representante legal, a não atribuição dos poderes e recursos necessários ao estabelecimento ou representante, e um conjunto de incumprimentos diretamente ligados às OEP e OEC, nomeadamente a não conservação ou não transmissão de dados dentro dos prazos fixados no Regulamento, bem como a não prestação de informação sobre a impossibilidade de cumprimento.

Já será considerada contraordenação grave (artigo 10.º, n.º 2) a não adoção das medidas técnicas e operacionais para garantir a confidencialidade e integridade das ordens e dos dados produzidos ou conservados.

As molduras sancionatórias são diversas, dependendo da infração concreta, da sua qualificação como muito grave ou grave, e da natureza jurídica – pessoa singular ou coletiva – do infrator.

Em todo o caso, e no que configura uma inovação relativamente ao Regulamento, são estabelecidas molduras subsidiárias para a eventualidade de ser impossível determinar o volume de negócios anual da pessoa coletiva infratora.

A negligência é punível com coima reduzida a metade (artigo 13.º).

Pode ainda ser aplicada, cumulativamente, a sanção acessória de interdição do exercício da atividade de prestador de serviços em território nacional por período máximo de dois anos (artigo 12.º), cujo desrespeito é cominado com o crime de desobediência qualificada.

O incumprimento persistente de um dever omitido pode ainda dar lugar a sanção pecuniária compulsória (artigo 14.º), de valor diário entre € 2.000 e € 100.000 para pessoas coletivas (€ 100 a € 500 para pessoas singulares), com um montante máximo de € 3.000.000 (€ 150,000 para pessoas singulares) e um período máximo de 30 dias.

A instauração e decisão dos processos de contraordenação cabe ao conselho de administração da ANACOM (artigo 15.º), a quem compete igualmente a fiscalização (artigo 16.º), sendo o produto das coimas repartido entre o Estado (60%) e a própria ANACOM (40%) (artigo 17.º).

O terceiro objetivo desta Proposta, não mencionado no relatório, parece ser, à revelia de qualquer exigência de transposição da Diretiva e do efeito direto de que goza o Regulamento, a

designação das autoridades nacionais de emissão e de execução das OEP e OEC, através do aditamento à Lei do Cibercrime dos artigos 26.º-A, 26.º-B e 26.º-C (artigo 20.º da proposta).

O artigo 26.º-B designa como autoridade emissora, competente para emitir, validar e transmitir OEP e OEC, a autoridade judiciária nacional com competência para a direção do processo na fase em que este se encontra, ressalvadas as competências do juiz de instrução para autorizar ou ordenar atos na fase de inquérito.

O artigo 26.º-C designa como autoridade de execução de uma OEP ou OEC a autoridade nacional com competência para executar a mesma medida de investigação em território nacional, sendo territorialmente competente a autoridade judiciária da comarca em cuja área deva ser executada a medida.

O artigo 26.º-A assegura, por sua vez, a aplicação supletiva das disposições da LCC às OEP e OEC, em tudo o que não contrarie o Regulamento, fixando a paridade de tratamento entre as ordens europeias e as ordens internas equivalentes.

O quarto objetivo – igualmente não declarado mas decorrente do modelo orgânico nacional de cooperação judiciária internacional – passa pela designação da Procuradoria-Geral da República como autoridade central para efeitos do Regulamento, designadamente para o exercício das competências previstas nos artigos 4.º, n.º 6, e 5.º, n.º 10, do Regulamento, o que é feito através do aditamento do n.º 5 ao artigo 21.º da Lei n.º 144/99, de 15 de Setembro (artigo 19.º da proposta). Esta solução é coerente com o modelo orgânico português e garante a interlocução institucional exigida pelo Regulamento perante a Comissão Europeia e as autoridades dos outros Estados-Membros.

VI. A CONVENÇÃO DAS NAÇÕES UNIDAS CONTRA O CIBERCRIME

1. Aprovação e entrada em vigor

Uma análise ao panorama da cooperação judiciária internacional em sede de cibercriminalidade e recolha de prova digital não podia estar completa sem uma referência à recente Convenção das Nações Unidas contra o Cibercrime, adotada pela Assembleia Geral das Nações Unidas em 24 de dezembro de 2024 e aberta à assinatura em Hanói, em 25 e 26 de outubro de 2025[47].

À data de elaboração deste artigo, mais de setenta países tinham já assinado a Convenção, bem como a própria Comissão Europeia em nome da União, e apenas três Estados haviam depositado o instrumento de ratificação. A sua entrada em vigor exige quarenta ratificações[48].

[47] A Convenção das Nações Unidas contra o Cibercrime foi adotada pela Assembleia Geral das Nações Unidas na sua Resolução 79/243, de 24 de dezembro de 2024, e aberta à assinatura na cerimónia de Hanói, em 25 e 26 de outubro de 2025. Portugal assinou a Convenção em 25 de outubro de 2025.

[48] Nos termos do artigo 65.º, n.º 1, da Convenção das Nações Unidas contra o Cibercrime, esta entra em vigor 90 dias após o depósito do quadragésimo instrumento de ratificação, aceitação, aprovação ou adesão. Até à presente data, apenas Azerbaijão, Vietname e Catar depositaram os instrumentos de ratificação:

2. Principais inovações em relação à Convenção de Budapeste

A Convenção das Nações Unidas assume um alcance explicitamente global, procurando alcançar países que, por razões políticas ou geográficas, não aderiram à Convenção de Budapeste. Em relação a esta última, apresenta um catálogo de incriminações substancialmente mais vasto, incorporando crimes que as evoluções tecnológicas e as práticas criminosas dos últimos vinte anos tornaram prementes, como sejam, a divulgação não consensual de imagens íntimas, o aliciamento ou manipulação para o cometimento de crimes sexuais contra crianças (*cyber grooming*), e o branqueamento de vantagens originadas com a prática de cibercrimes.

Importa igualmente destacar que a Convenção da ONU incorpora, pela primeira vez numa convenção de alcance global, disposições específicas sobre perda de vantagens do crime e recuperação internacional de ativos provenientes de crimes informáticos (artigo 49.º), colmatando uma lacuna da Convenção de Budapeste.
Inclui também disposições específicas sobre proteção de dados (artigo 36.º), refletindo as evoluções ocorridas desde a Convenção de Budapeste, muito anterior ao Regulamento Geral sobre a Proteção de Dados.

3. Críticas e tensões

A Convenção da ONU não foi aprovada sem controvérsia. Organizações representativas do setor tecnológico, como o Cybersecurity Tech Accord[49], expressaram preocupações sobre o facto de a Convenção utilizar conceitos amplos que poderiam, na prática, legitimar formas de vigilância digital invasiva ou, através dos canais de cooperação estabelecidos, viabilizar o intercâmbio de dados pessoais com países que não oferecem garantias equivalentes de proteção dos direitos humanos.

A crítica central é que a Convenção, ao ambicionar incluir países com conceções muito distintas sobre o papel do Estado na esfera privada dos cidadãos, sob o desígnio da maior amplitude e universalidade possíveis, acaba por sacrificar a exigência de requisitos mínimos em sede de Estado de Direito e respeito por direitos individuais.

Estas preocupações não são frívolas ou infundadas. A aplicação concreta da Convenção dependerá em larga medida das declarações interpretativas que os Estados emitam aquando da ratificação, do modo como os respetivos tribunais interpretem as suas disposições, e da efetividade das salvaguardas de direitos humanos previstas no artigo 6.º da Convenção[50].

(https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en).

[49] Sobre os riscos identificados por organizações da sociedade civil e do setor tecnológico, v. Cybersecurity Tech Accord, «Press Release: Calls for changes to new UN treaty to prevent damage to global security online», outubro de 2025, disponível em https://cybertechaccord.org; e Electronic Frontier Foundation, «The UN Cybercrime Treaty: A Threat to Human Rights and Internet Freedom», agosto de 2023.

[50] Sob a epígrafe "Respect for human rights", reza o artigo 6.º: «*1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law. 2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of*

VII. PROBLEMAS TRANSVERSAIS NÃO RESOLVIDOS

Pese embora todos os esforços no sentido da multiplicação de instrumentos jurídicos com vista a regular, agilizar e harmonizar a cooperação judiciária em sede de combate ao cibercrime e à recolha de prova digital em contexto transfronteiriço, e independentemente da avizinhada confluência de todos estes instrumentos, são apontados, por alguns autores problemas de natureza jurídica e técnica, que poderão, se não frustrar, pelo menos dificultar bastante a consecução dos objetivos que os próprios instrumentos aqui analisados declaram pretender atingir.

1. O problema da encriptação: «the going dark problem»

A expressão «*going dark problem*», cunhada na literatura anglo-saxónica[51], designa o fenómeno pelo qual a proliferação da encriptação de ponta a ponta progressivamente torna inacessível, mesmo às autoridades judicialmente autorizadas, o conteúdo das comunicações.

O mecanismo funciona da seguinte maneira: os prestadores de serviços apenas têm acesso aos dados encriptados que armazenam, uma vez que a chave de desencriptação pertence exclusivamente ao utilizador, pelo que, ao executarem uma OEP, apenas podem entregar às autoridades ordenantes informação cifrada, sem utilidade probatória imediata.

Nenhum dos instrumentos analisados neste artigo resolve este problema. O Regulamento regula a transmissão de dados armazenados, mas não impõe aos prestadores destinatários das OEP qualquer obrigação no sentido de os transmitir em formato legível.

A um nível interno, existem respostas legislativas de diversa índole.

A Irlanda optou por impor aos prestadores a obrigação de fornecer os dados em formato legível, ao passo que a França seguiu um caminho diferente, criminalizando a recusa de entrega da chave de desencriptação quando tal seja judicialmente ordenado[52].

Em Portugal, tanto quanto se alcança, esta questão permanece sem resposta legislativa[53], o que constitui uma lacuna que o pacote *e-evidence* deliberadamente não vem suprir[54].

---

expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.»

[51] O «going dark problem» é a expressão utilizada para descrever a dificuldade das autoridades em aceder ao conteúdo de comunicações encriptadas de ponta a ponta (end-to-end encryption), mesmo quando detêm uma autorização judicial válida. Para uma análise aprofundada do problema, v. Stefan Bellovin et al., «Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications», Journal of Cybersecurity, vol. 1, 2015, pp. 69-79.

[52] Tozsa, *op. cit.* p. 251.

[53] Não confundir, obviamente, com a criminalização do desrespeito da sanção acessória de interdição do exercício da atividade de prestador de serviços em território nacional, proposta no artigo 12.º, n.º 3 da Proposta de Lei n.º 83/XVII/1.ª.

[54] Nos precisos termos do considerando 20 do Regulamento «*A aplicação do presente regulamento não deverá afetar a utilização da encriptação pelos prestadores de serviços ou pelos seus utilizadores. Os dados solicitados através de uma ordem europeia de produção ou de uma ordem europeia de conservação*

Cumprindo notar, a este respeito, que o artigo 14.º da LCC, que prevê a injunção para apresentação ou concessão de acesso a dados, não oferece aqui uma resposta útil, pois impõe um dever de disponibilização de dados que a pessoa já detenha ou a que tenha acesso, não um dever de decifração de dados que o destinatário da ordem seja tecnicamente incapaz de ler.

2. A admissibilidade e valoração processual da prova digital obtida no estrangeiro

O pacote legislativo europeu regula os mecanismos de obtenção de prova digital, mas não harmoniza as regras de produção e valoração probatória nos processos penais nacionais.

A questão de saber em que condições uma prova digital obtida através de uma OEP pode ser valorada pelo tribunal, e quais os requisitos formais do seu ingresso num processo judicial, fica inteiramente remetida ao direito processual penal de cada Estado-Membro.

A experiência recente com as provas obtidas a partir da plataforma EncroChat[55] ilustra os riscos deste estado de fragmentação: tribunais de diferentes Estados-Membros chegaram a conclusões opostas sobre a admissibilidade dos mesmos dados, gerando incerteza jurídica e potencial violação do princípio da igualdade dos arguidos em processos conexos.

O risco de um «EncroChat all over again» com as provas obtidas através das futuras OEP é real e não deve ser subestimado.

3. A coexistência de regimes paralelos e a escolha do instrumento mais adequado

Nenhum dos novos instrumentos revoga ou substitui os anteriores. O Regulamento (UE) 2023/1543 coexiste com a Decisão Europeia de Investigação (DEI), com os mecanismos da Convenção de Budapeste, com os acordos bilaterais de auxílio judiciário mútuo e com as cartas rogatórias tradicionais. Esta sobreposição é uma fonte potencial de complexidade para as autoridades judiciárias, que terão de escolher, em cada caso concreto, o instrumentomais adequado tendo em conta a natureza dos dados pretendidos, a localização do prestador, a urgência da diligência e as garantias de defesa do arguido.

---

deverão ser fornecidos ou conservados independentemente de estarem ou não encriptados. No entanto, o presente regulamento não deverá impor a obrigação de decifrar os dados aos prestadores de serviços.».

[55] O caso EncroChat, em que a infiltração policial coordenada pela Europol permitiu desencriptar milhões de mensagens trocadas numa plataforma de comunicação utilizada por redes criminosas, gerou intensa controvérsia jurisprudencial em vários Estados-Membros da UE. O marco jurisprudencial decisivo sobre a admissibilidade dos dados EncroChat nos sistemas penais europeus é o Acórdão do TJUE (Grande Secção) de 30 de abril de 2024, Processo C-670/22, Staatsanwaltschaft Berlin v. M.N., que determinou que uma DEI que solicite provas já detidas pelo Estado de execução deve ser emitida pela autoridade competente nos termos do direito interno do Estado emitente e satisfazer os requisitos de proporcionalidade, mas deixou à apreciação dos tribunais nacionais a questão da validade processual dos dados assim obtidos, o que perpetua a fragmentação identificada no texto. Para análise doutrinária, v. Jan-Jaap Oerlemans / Dave van Toor, «Legal Aspects of the EncroChat Operation: A Human Rights Perspective», European Journal of Crime, Criminal Law and Criminal Justice, vol. 30 (3-4), 2022, pp. 309-328; e G. Sagittae, «On the lawfulness of the EncroChat and Sky ECC- operations», New Journal of European Criminal Law, vol. 14(3), 2023, pp. 269-272.

Alguns dos dilemas mais difíceis surgem precisamente nos casos de sobreposição de âmbito entre instrumentos. Se a DEI, aplicada à recolha de prova em suporte eletrónico, oferece maiores garantias de contraditório e de controlo do Estado de execução do que a OEP, qual a consequência processual da opção pela via mais célere mas menos garantística?

Será que a OEP, por ser um instrumento mais intrusivo nos direitos do suspeito, deve estar sujeita a um controlo judicial mais exigente no Estado de emissão? São perguntas às quais a doutrina e a jurisprudência europeias terão de dar resposta nos próximos anos.

VIII. CONCLUSÕES

O panorama que resulta da análise aqui empreendida é o de um quadro normativo em acelerada transformação, movido pela consciência coletiva de que os instrumentos tradicionais de cooperação judiciária foram superados pela velocidade e pela ubiquidade da prova digital. Os novos instrumentos – o pacote e-evidence europeu, o Segundo Protocolo Adicional à Convenção de Budapeste, a Convenção da ONU – representam avanços significativos que merecem acolhimento positivo.

Contudo, a ambição normativa não basta. Instrumentos juridicamente sofisticados que não sejam acompanhados de infraestruturas técnicas operacionais, de autoridades competentes devidamente identificadas e formadas, e de regras processuais nacionais que assegurem a admissibilidade e o valor probatório das provas obtidas, arriscam transformar-se em letra morta ou, pior, em fonte de incerteza jurídica.

As conclusões que se impõem são, portanto, de ordem prática tanto quanto normativa: a aprovação da Proposta de Lei n.º 83/XVII/1.ª – ou de outra que a substitua, transpondo a Diretiva – e a designação das autoridades competentes é urgente, a formação especializada das magistraturas é indispensável e a questão da encriptação de ponta a ponta e da admissibilidade processual da prova digital obtida no estrangeiro requer atenção legislativa específica que os instrumentos analisados não providenciam.

Num domínio em que a cooperação eficaz pode ser a diferença entre o sucesso e o insucesso de investigações criminais de enorme gravidade – ataques a infraestruturas críticas, crimes de abuso sexual infantil online, ataques de *ransomware* a hospitais – o investimento em recursos humanos e técnicos é, em última análise, também um investimento na proteção dos direitos dos cidadãos e no Estado de Direito.

LEGISLAÇÃO, INSTRUMENTOS NORMATIVOS E JURISPRUDÊNCIA

I. Direito nacional (Portugal)

Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), alterada pela Lei n.º 79/2021, de 24 de novembro – Diário da República, 1.ª Série, n.º 180, 15 de setembro de 2009

Lei n.º 59/2019, de 8 de agosto – transposição da Diretiva (UE) 2016/680 (proteção de dados pelas autoridades competentes para efeitos penais)

Lei n.º 144/99, de 31 de agosto (cooperação judiciária internacional em matéria penal), na redação atual

Lei n.º 16/2022, de 16 de agosto (Lei das Comunicações Electrónicas)

Lei n.º 88/2017, de 21 de agosto (regime jurídico da emissão, transmissão, reconhecimento e execução de decisões europeias de investigação em matéria penal)
Lei n.º 99/2009, de 4 de setembro (regime quadro das contraardenações do sector das comunicações)

Decreto-Lei n.º 30/2020, de 29 de junho

Resolução da Assembleia da República n.º 88/2009, de 15 de setembro (aprovação da Convenção sobre o Cibercrime)

Decreto do Presidente da República n.º 91/2009, de 15 de setembro (ratificação da Convenção sobre o Cibercrime) – Diário da República, 1.ª Série, n.º 179, 15 de setembro de 2009

Proposta de Lei n.º 83/XVII/1.ª (transposição da Diretiva (UE) 2023/1544 e regime sancionatório do Regulamento (UE) 2023/1543), aprovada em Conselho de Ministros de21 de maio de 2026, admitida na Assembleia da República em 2 de junho de 2026

II. Direito da União Europeia

Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova electrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais – JO L 191, 28 de julho de 2023, pp. 118-180

Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova electrónica em processos penais – JO L 191, 28 de julho de 2023, pp. 181-198

Regulamento de Execução (UE) 2025/1550 da Comissão, de 28 de julho de 2025, que estabelece as especificações técnicas e outros requisitos para o sistema informático descentralizado referido no Regulamento (UE) 2023/1543 – JO L 2025/1550, 18 de agosto de 2025

Decisão do Conselho (UE) 2023/436, de 14 de fevereiro de 2023, que autoriza os Estados-Membros a ratificarem o Segundo Protocolo Adicional à Convenção sobre o Cibercrime (STE n.º 224) – JO L 63, 28 de fevereiro de 2023, pp. 48-53

Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal – JO L 130, 1 de maio de 2014, p. 1

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais – JO L 119, 4 de maio de 2016, p. 89

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados) – JO L 119, 4 de maio de 2016, p. 1

Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação – JO L 69, 16 de março de 2005, p. 67

Decisão-Quadro 2002/465/JAI do Conselho, de 13 de junho de 2002, relativa às equipas de investigação conjunta – JO L 162, 20 de junho de 2002, p. 1

Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação – JO L 218, 14 de agosto de 2013, p. 8

Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo – JO L 88, 31 de março de 2017, p. 6

Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil – JO L 335, 17 de dezembro de 2011, p. 1

Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário – JO L 123, 10 de maio de 2019, p. 18

Comissão Europeia, Documento de Trabalho dos Serviços da Comissão – Avaliação de Impacto, SWD(2018) 118 final, de 17 de abril de 2018 – EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018SC0118

Proposta de Regulamento COM(2018) 225 final, de 17 de abril de 2018 – EUR-Lex:

https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?qid=1550155986946&uri=CELEX:52018PC0225&from=EN

III. Direito internacional convencional

Convenção sobre o Cibercrime (STE n.º 185), aberta à assinatura em Budapeste em 23 de novembro de 2001, em vigor desde 1 de julho de 2004 – Conselho da Europa

Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e à divulgação de provas electrónicas (STE n.º 224), adotado em 17 de novembro de 2021, aberto à assinatura em 12 de maio de 2022 – Conselho da Europa

Convenção das Nações Unidas contra o Cibercrime, adotada pela Assembleia Geral das Nações Unidas na Resolução 79/243, de 24 de dezembro de 2024, aberta à assinatura em Hanói em 25 e 26 de outubro de 2025
Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, de 20 de abril de 1959 – Conselho da Europa

Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia – JO C 197, 12 de julho de 2000, p. 3

IV. Documentos do Comité da Convenção sobre o Cibercrime (T-CY)

Conselho da Europa, T-CY, Guidance Note #3 on Transborder Access to Data (Article 32), T-CY(2014)25, 3 de dezembro de 2014 – https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf

Conselho da Europa, T-CY, Transborder Access and Jurisdiction: What are the Options?, T-CY(2012)3, adotado na 8.ª Plenária do T-CY, 6 de dezembro de 2012

V. Jurisprudência

Tribunal de Justiça da União Europeia (Grande Secção), Acórdão de 30 de abril de 2024, Processo C-670/22, Staatsanwaltschaft Berlin v. M.N. (EncroChat) EUR-Lex - 62022CJ0670 - EN - EUR-Lex

REFERÊNCIAS BIBLIOGRÁFICAS

ABELSON, Harold / ANDERSON, Ross / BELLOVIN, Steven M. / BENALOH, Josh / BLAZE, Matt / DIFFIE, Whitfield / GILMORE, John / GREEN, Matthew / LANDAU, Susan / NEUMANN, Peter G. / RIVEST, Ronald L. / SCHILLER, Jeffrey I. / SCHNEIER, Bruce / SPECTER, Michael A. / WEITZNER, Daniel J., «Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications», Journal of Cybersecurity, vol. 1, n.º 1, 2015, pp. 69-79, DOI: 10.1093/cybsec/tyv009

CYBERSECURITY TECH ACCORD, «Press Release: Calls for changes to new UN treaty to prevent damage to global security online», outubro de 2025 – https://cybertechaccord.org

DE JONGE, Boudewijn / DE VRIES, Barry, «Data-Driven Investigations in a Cross-Border Setting», eucrim, Vol. 19(3), 2024, pp. 214-221, DOI: 10.30709/eucrim-2024-020

ELECTRONIC FRONTIER FOUNDATION, «The UN Cybercrime Treaty: A Threat to Human Rights and Internet Freedom», agosto de 2023 Joint Statement on the UN Cybercrime Convention: EFF and Global Partners Urge Governments Not to Sign | Electronic Frontier Foundation

EUROJUST, Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers, janeiro de 2024

Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers | Eurojust | European Union Agency for Criminal Justice Cooperation

GLESS, Sabine / RICHTER, Thomas (eds.), Do Exclusionary Rules Ensure a Fair Trial?, Intersentia, 2019
Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules | Springer Nature Link

KOOPS, Bert-Jaap / GOODWIN, Morag, «Cyberspace, the Cloud, and Cross-Border Criminal Investigation – The limits and possibilities of International Law», Tilburg Institute for Law, Technology, and Society / CTLD, dezembro de 2014 – https://repository.wodc.nl/server/api/core/bitstreams/6fa89957-53ac-4358-939d-4681d1b404a0/content

LINDEMAN, Joep / LUCHTMAN, Michiel / VAN TOOR, Dave (eds.), Admissibility of Evidence in EU Cross-Border Criminal Proceedings, 2024 – https://dspace.library.uu.nl/items/9f7e62aa-cb24-43f2-892d-b0d3c3fa04c6
Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands

OERLEMANS, Jan-Jaap / VAN TOOR, Dave, «Legal Aspects of the EncroChat Operation: A Human Rights Perspective», European Journal of Crime, Criminal Law and Criminal Justice, vol. 30 (3-4), 2022, pp. 309-328

Legal Aspects of the EncroChat Operation: A Human Rights Perspective in: European Journal of Crime, Criminal Law and Criminal Justice Volume 30 Issue 3-4 (2022)

SAGITTAE, Georgios, «On the lawfulness of the EncroChat and Sky ECC-operations», New Journal of European Criminal Law, vol. 14, n.º 3, 2023, pp. 273-293, DOI: 10.1177/20322844231159576

TOSZA, Stanisław, «Electronic Evidence after the E-Evidence Package's Adoption: Challenges for Application and Unresolved Problems», Studia Iuridica Lublinensia, vol. 33, n.º 5, 2024, pp. 237-260, DOI: 10.17951/sil.2024.33.5.237-260

VERDELHO, Pedro, «A nova Lei do Cibercrime», Scientia Iuridica, Outubro-Dezembro 2009, Tomo LVIII – Número 320, Braga, 2009, pp. 733-735

WEIGEND, Thomas, «The Potential to Secure a Fair Trial Through Evidence Exclusion: A German Perspective», in Do Exclusionary Rules Ensure a Fair Trial? (Sabine Gless / Thomas Richter, eds.), Intersentia, 2019, pp. 61-88 – https://lgcl.csl.mpg.de/attachments/Weigend_2019_The_potential_to_secure_a_fair_trial_through_evidence_exclusion.pdf

Vídeo da intervenção

https://educast.fccn.pt/vod/clips/2pzj8dsrfv/streaming.html?locale=pt

4. QUESTÕES RELEVANTES EM SEDE DE ACESSO A METADADOS APÓS A LEI N.º 18/24, DE 5 DE FEVEREIRO[1]

Rui Cardoso*

Vídeo da intervenção

https://educast.fccn.pt/vod/clips/2pzj8dss0s/streaming.html?locale=pt

[1] Comunicação do autor no Seminário «Cibercrime e e-evidence», realizado em Lisboa, em 20 de abril de 2026, no Centro de Estudos Judiciários.

* Procurador-Geral Adjunto, Diretor do DCIAP.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

ANEXOS

Os ficheiros estão em PDF. O tamanho pode ir até aos 12 MG.

- Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime);
- Convenção Sobre o Cibercrime (Convenção de Budapeste);
- Segundo Protocolo Adicional à Convenção de Budapeste;
- Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho de 12 de julho de 2023;
- Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho de 12 de julho de 2023
- Proposta de Lei n.º 83/XVII/1.ª;
- *United Nations Office on Drugs and Crime* United Nations Convention against Cybercrime [Consultado em 30 de junho de 2026];
- Lei n.º 32/2008, de 17 de julho.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Título:
Cibercrime e *e-evidence*

Ano de Publicação: 2026

ISBN: 978-989-9102-43-9

Coleção: Formação Contínua

Edição: Centro de Estudos Judiciários
Largo do Limoeiro
1149-048 Lisboa
cej@mail.cej.mj.pt