COLEÇÃO FORMAÇÃO CONTÍNUA

CIBERCRIMINALIDADE E PROVA DIGITAL

JURISDIÇÃO PENAL E PROCESSUAL PENAL

JULHO 2018

Edição atualizada em maio 2020

CENTRO DE ESTUDOS JUDICIÁRIOS

Diretor do CEJ
João Manuel da Silva Miguel, Juiz Conselheiro

Diretores Adjuntos
Paulo Alexandre Pereira Guerra, Juiz Desembargador
Luís Manuel Cunha Silva Pereira, Procurador-Geral Adjunto

Coordenador do Departamento da Formação
Edgar Taborda Lopes, Juiz Desembargador

Coordenadora do Departamento de Relações Internacionais
Helena Leitão, Procuradora da República

Grafismo
Ana Caçapo - CEJ

Capa
Edifício do CEJ

Foto
Victor Pimenta - CEJ

O Direito relativo à criminalidade relacionada com o mundo digital tem trazido nos últimos anos novos problemas que a ciência jurídica e, em concreto, os tribunais têm vindo a resolver.

A aquisição da prova é um momento essencial do processo penal mas também, e por isso mesmo, das garantias fundamentais dos cidadãos.

O debate vem sendo acompanhado e também promovido nas acções de formação do Centro de Estudos Judiciários[1] e este novo e-book da "Coleção Formação Contínua" vem dar-lhe seguimento.

A reflexão é essencial, a inquietação é necessária e, assim, as pistas de solução irão surgir (num contexto que só pode passar pelo respeito do direito constitucional).

O e-book, completa-se agora (em Maio de 2020, com um novo texto da Professora e Advogada Raquel Brízida Castro, que resume a sua intervenção em Fevereiro de 2019, nos "Temas de Direito Penal 2018-2019), onde aborda a temática do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou execução de sanções penais, tudo em ligação com o regime de protecção de dados e da Directiva UE2016/680.

Este pequeno texto – elaborado em Janeiro deste ano – serve de guia para a matéria e encontra no e-book que agora se actualiza o campo perfeito de utilidade para quem tem de com ela lidar.

(ETL)

[1] *Vide* "O domínio do imaterial: prova digital, cibercrime e a tutela penal de direitos intelectuais".

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Ficha Técnica

Nome:

Cibercriminalidade e Prova Digital

Jurisdição Penal e Processual Penal:

Helena Susano – Juíza de Direito, Docente do CEJ e Coordenadora da Jurisdição
José Quaresma – Juiz de Direito e Docente do CEJ
Alexandre Au-Yong de Oliveira – Juiz de Direito e Docente do CEJ
Rui Cardoso – Procurador da República e Docente do CEJ
Susana Figueiredo – Procuradora da República e Docente do CEJ
Patrícia Naré Agostinho – Procuradora da República e Docente do CEJ
Miguel Rodrigues – Procurador da República e Docente do CEJ

Coleção:

Formação Contínua

Plano de Formação 2014/2015:

Cibercriminalidade – 14 de março de 2014 (programa)

Plano de Formação 2015/2016:

Prova em Direito Penal, cibercriminalidade e prova em ambiente digital – 7 e 8 de abril de 2016 (programa)

Plano de Formação 2016/2017:

Temas de Direito Penal e Processual Penal – 3 e 10 de fevereiro e 3 e 10 de março de 2017 (programa)

Plano de Formação 2018/2019:

Temas de Direito Penal e Processual Penal – 8 e 15 de fevereiro e 8 e 15 de março de 2019 (programa)

Conceção e organização:

Jurisdição Penal e Processual Penal

Intervenientes:

Carlos Nunes – Inspetor da Polícia Judiciária
David Silva Ramalho – Advogado
Fernanda Pêgo – Procuradora da República, Coordenadora no Departamento de Investigação e Ação Penal de Lisboa
João Conde Correia – Procurador da República
Manuel David Masseno – Professor do Instituto Politécnico de Beja
Pedro Verdelho, Procurador da República – Coordenador do Gabinete Cibercrime da PGR
Raquel Alexandra Brízida Castro – Professora da Faculdade de Direito da Universidade de Lisboa
Rui Cardoso – Procurador da República e Docente do Centro de Estudos Judiciários

Revisão final:
Edgar Taborda Lopes – Juiz Desembargador, Coordenador do Departamento da Formação do CEJ
Ana Caçapo – Departamento da Formação do CEJ

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

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

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

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

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
1.ª edição –27/07/2018	17/06/2019
	13/05/2020

Cibercriminalidade e Prova Digital

Índice

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1.

Proteção de Dados e a Diretiva UE2016/680

Raquel Alexandra Brízida Castro

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1. PROTEÇÃO DE DADOS E A DIRETIVA UE2016/680: O TRATAMENTO DE DADOS PESSOAIS PELAS AUTORIDADES COMPETENTES PARA EFEITOS DE PREVENÇÃO, INVESTIGAÇÃO, DETEÇÃO OU REPRESSÃO DE INFRAÇÕES PENAIS OU EXECUÇÃO DE SANÇÕES PENAIS[1]

Raquel Alexandra Brízida Castro*

1. A regulação do ciberespaço tem, atualmente, de enfrentar um verdadeiro emaranhado regulatório, normativo e institucional[2]. Em matéria de proteção de dados, a fragmentação jurídica mencionada, gerada pela produção normativa da União Europeia, agudiza-se perante a, surpreendente, multiplicidade de leis nacionais aplicáveis, somada à abundância de autoridades de controlo do ciberespaço competentes, mais ou menos prósperas em termos jurídicos.

2. Efetivamente, no plano normativo, apenas em sede de proteção de dados, cabe destacar os seguintes instrumentos jurídicos da União Europeia vigentes:

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);

- 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 ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (Doravante DPD;

- Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

- Regulamento (CE) n.º 45/2001 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

Em termos nacionais, a legislação europeia referida gerou, direta ou indiretamente – voluntária ou involuntariamente –, os seguintes atos legislativos nacionais:

[1] Apresentação decorrida na ação de formação "Temas de Direito Penal e Processual Penal", no CEJ, nos dias 8, 15 de fevereiro e 8, 15 de março de 2019.

* Professora da Faculdade de Direito da Universidade de Lisboa.

[2] Para uma descrição e análise exaustiva dessa dispersão regulatória, normativa e institucional, numa perspetiva jurídico-constitucional: BRÍZIDA CASTRO, Raquel (2019) "Regulação do Ciberespaço: Projeções Constitucionais do novo Paradigma Jurídico-Público Regulatório", *in Garantia de Direitos e Regulação: Perspectivas de Direito Administrativo;* Coord. Carla Amado Gomes, Rute Saraiva, Ricardo Pedro e Fernanda Maçãs; pp. 367-412.

a) Atos de execução do RGPD:

- Lei de Execução RGPD – Lei n.º 58/2019, de 8 de agosto;

- Decreto que resultou da Proposta de Lei n.º 126/XIII, que altera Lei n.º 34/2009, de 14 de julho, que estabelece o regime aplicável ao tratamento de dados referentes ao sistema judicial;

b) Outros:

- Lei n.º 59/2019, de 8 de agosto – que transpõe a Diretiva (UE) 2016/680, 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 ou execução de sanções penais;

- Lei n.º 21/2019, de 21 de Fevereiro, que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e procede à terceira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna – Lei de Transposição da Diretiva PNR.

Convém, ainda, referir outros regimes relativos ao tratamento de dados pessoais pelos órgãos de polícia criminal e pelas autoridades judiciárias, como a Lei n.º 83/2017, de 28 de agosto, que estabelece medidas de natureza preventiva e repressiva de combate ao branqueamento de capitais e ao financiamento do terrorismo. São as autoridades judiciárias e os órgãos de policia criminal (além das «entidades obrigadas») autorizadas a tratar várias categorias de dados financeiros e outros que se mostrem relevantes para a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo, sendo esse tratamento considerado feito num domínio de proteção de um interesse público importante, para efeitos dos regimes de proteção de dados.

3. No que se refere à dispersão regulatória institucional, à Comissão Nacional de Proteção de Dados (doravante CNPD)[3], caberia somar as autoridades de controlo, recém-criadas, transfiguradas ou a recuperar, criadas no âmbito dos seguintes instrumentos normativos:

i) O Decreto que estabelecia o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial[4]; e

[3] Cf. Artigo 3.º da Lei n.º 58/2019 de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[4] O Decreto que resultou da Proposta de Lei n.º 126/XIII foi, entretanto, objeto de veto presidencial.

ii) A Lei que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) n.º 2016/680[5].

3.1. Quanto à Lei de Execução do RGPD para o sistema judicial, no Decreto que resultou da Proposta de Lei nº 126/XIII, o legislador conferia aos magistrados judiciais e do MP a responsabilidade pelo tratamento de dados no âmbito de processos da sua competência, e excluía, expressamente, a CNPD da supervisão do tratamento efetuado no exercício das funções e competências processuais dos tribunais e do Ministério Público.

Ora, o diploma, objeto de veto presidencial, ressuscitava a Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial, que passaria a designar-se *Comissão de Coordenação da Gestão da Informação do Sistema Judiciário*. Esta Comissão teria uma nova composição e competências acrescidas. Na fundamentação preambular do legislador, o objetivo seria *"prevenir a intervenção de uma autoridade administrativa no exercício de funções judiciais, assegurando-se o respeito pela independência dos tribunais e pela autonomia do Ministério Público*".

Porém, a versão que vingou – mas que soçobrou perante o veto presidencial – mereceu críticas severas do Conselho Superior da Magistratura (CSM). Vale a pena recuperar tais desfeitas, sobretudo em dois tópicos explosivos[6]:

a) O CSM veio questionar a identificação da atividade jurisdicional dos juízes, relativa ao tratamento de dados pessoais nos processos judiciais, como de responsável pelo tratamento[7]. Note-se que, no exercício dessa atividade, os juízes não determinam os meios – disponibilizados e geridos pelo Ministério da Justiça – nem as finalidades, que são estabelecidas por lei. Destarte, perante o regime da responsabilidade civil extracontratual do Estado e demais entidades públicas (Lei n.º 67/2007), como

[5] Cf. Lei n.º 59/2019 de 8 de agosto.

[6] http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449324c56684a53556c664d5335775a47593d&fich=ppl126-XIII_1.pdf&Inline=true

[7] *Artigo 23.º*
1 - Para efeitos do disposto nos regimes de proteção de dados pessoais, são responsáveis pelo tratamento de dados:
a) Os magistrados judiciais e do Ministério Público competentes, nos termos da lei do processo, relativamente aos dados tratados no âmbito e em atos do processo, no exercício da sua atividade processual e sob a sua direção ou autoridade;
b) Os juízes de paz e os mediadores dos sistemas públicos de mediação, relativamente aos dados pessoais tratados no âmbito dos respetivos processos;
c) As entidades supervisoras da gestão da informação a que se refere o Artigo seguinte, relativamente a outras operações de tratamento.
2 - No que se refere aos dados pessoais no processo, as entidades responsáveis pelo tratamento de dados pessoais, nos termos das alíneas a) e b) do número anterior, asseguram a efetiva proteção dos direitos de informação, de acesso e de retificação ou apagamento dos dados, nos termos dos regimes de proteção de dados pessoais, por sua iniciativa ou mediante requerimento do respetivo titular.
3 - O Ministério Público é o responsável pelo tratamento dos dados previstos no Artigo 9.º, designadamente para efeitos do número anterior.
4 - Quando prossigam as finalidades previstas no Artigo 33.º, consideram-se responsáveis pelo tratamento as entidades nele indicadas, designadamente para efeitos de cumprimento das obrigações previstas no n.º 2 do presente Artigo.

interpretar os Artigos relativos aos meios de tutela e de responsabilidade e ao direito, referido na lei, de obter indemnização do responsável pelo tratamento?

b) O Decreto atribuía as competências de autoridade de controlo à *Comissão de Coordenação das Gestão da Informação do Sistema Judiciário*, cujos órgãos seriam presididos por membros do governo da área da justiça[8]. Em acréscimo, o respetivo conselho coordenador integraria representantes de órgãos administrativos dependentes, diretamente, do governo[9]. Apesar da advertência, prudente, do CSM de que esta solução constitui uma ostensiva violação do princípio da separação de poderes, a versão final da lei manteve a solução.

Conforme assinalado, o Decreto em apreço foi devolvido ao Parlamento, nos termos constitucionais, tendo o Presidente da República considerado que o modelo escolhido pelo legislador – de autoridade de controlo e de autoridade de coordenação – não garantia o cumprimento, na ordem jurídica interna, do RGPD, quanto às áreas específicas de funções dos Tribunais, no exercício da independência da função jurisdicional, e do Ministério Público, no desempenho, com autonomia, das suas funções e competências processuais[10]. Na mensagem endereçada à Assembleia da República, o Presidente lembra, igualmente, que o regime imposto pelo RGPD, e que a lei não cumpre, é *"por sinal consonante com a Constituição da República Portuguesa*".

Não tendo o Parlamento procedido à confirmação do Decreto controvertido[11], nem introduzido quaisquer alterações, a iniciativa caducou com o termo da legislatura, em 2019, por imposição constitucional.

3.2. Por sua vez, na Lei 59/2019 – ato legislativo que veio transpor a Diretiva 2016/680 –, o legislador atribui à CNPD a garantia e fiscalização do seu cumprimento, exceto no tratamento de dados pessoais efetuado pelos tribunais e pelo Ministério Público no exercício das suas competências processuais. A CNPD adquire uma nova composição, pois passa a integrar um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público.

Acresce o papel de autoridade de controlo que lhe é atribuído pela Lei n.º 21/2019, ato legislativo interno que transpõe a designada Diretiva PNR.

[8] De acordo com a alínea a), do n.º 4, do Artigo 25.º, referente à composição da Comissão de Coordenação da Gestão da Informação do Sistema Judiciário, o conselho superior da Comissão é constituído pelo membro do Governo responsável pela área da justiça, que preside. Por sua vez, nos termos do n.º 6, o conselho coordenador é presidido pelo membro do Governo com competências no âmbito dos sistemas de informação dos tribunais ou por seu representante.
[9] Representantes designados pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I. P.; Direção-Geral da Administração da Justiça; Secretaria-geral do Ministério da Justiça e Direcção-Geral da Política de Justiça. Sempre que devam ser apreciados assuntos relacionados com o tratamento de dados por que sejam responsáveis: Um representante designado pela Direção-Geral de Reinserção e Serviços Prisionais e um representante de cada um dos órgãos de polícia criminal.
[10] https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42506
[11] Cf. Artigo 136.º, n.º 2, da CRP.

4. Por fim, a título introdutório do registo da presente intervenção, cabe destacar algumas incontornáveis diferenças de regime da Diretiva 2016/680 em relação ao RGPD, em especial no que se refere ao exercício dos direitos dos titulares dos dados.

Em sede da Diretiva 2016/680, as finalidades que legitimam o tratamento dos dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, revestem um peso considerável na inelutável ponderação com os direitos dos titulares dos dados pessoais objeto de tratamento, salvo casos patológicos.

A título meramente exemplificativo, a propósito das informações a disponibilizar ou a fornecer pelo responsável pelo tratamento (Cf. Artigo 14.º), note-se que a prestação de informações (adicionais) pode ser adiada, limitada ou recusada se, e enquanto, tal for necessário e proporcional para: evitar prejuízo para investigações, inquéritos ou processos judiciais; para a prevenção, deteção, investigação ou repressão de infrações penais ou para a execução de sanções penais; ou ainda para proteger a segurança pública, a segurança nacional ou proteger os direitos, liberdades e garantias de terceiros (Cf. Artigo 14.º, n.º 3).

Com os mesmos fundamentos, pode o responsável pelo tratamento recusar ou restringir o direito de acesso do titular dos dados, enquanto tal limitação constituir uma medida necessária e proporcional (Cf. Artigo 16.º). Nestes casos, o responsável pelo tratamento informa o titular dos dados, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso. Tal informação apenas pode ser omitida se prejudicar uma das finalidades referidas. Cabe ainda ao responsável pelo tratamento disponibilizar à autoridade de controlo informação sobre os motivos de facto e de direito que fundamentam a decisão de recusa ou de limitação do direito de acesso, bem como da omissão de informação ao titular dos dados.

Sublinhe-se ainda, neste conspecto, a configuração do direito de retificação ou apagamento dos dados pessoais e de limitação do tratamento (Cf. Artigo 17.º). Em vez de proceder ao apagamento, o responsável pelo tratamento limita o tratamento, no caso de: a) O titular dos dados contestar a exatidão dos dados pessoais e a sua exatidão ou inexatidão não puder ser apurada; b) Os dados pessoais deverem ser conservados para efeitos de prova. Nestes casos, os dados só podem ser tratados para as finalidades que impediram o seu apagamento, devendo o responsável pelo tratamento adotar as medidas técnicas e organizativas adequadas para assegurar que a limitação é respeitada.

Lisboa, 13 de janeiro de 2020

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/1b5lli4bd/streaming.html?locale=pt

2.

Reflexões sobre o impacto das Novas Tecnologias na Interpretação e Justiça Constitucional

Raquel Alexandra Brízida Castro

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2. REFLEXÕES SOBRE O IMPACTO DAS NOVAS TECNOLOGIAS NA INTERPRETAÇÃO E JUSTIÇA CONSTITUCIONAL[1]

Raquel Alexandra Brízida Castro*

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/13vwtviahd/flash.html?locale=pt

[1] Apresentação decorrida na ação de formação "Prova em Direito Penal, cibercriminalidade e prova em ambiente digital", no CEJ, nos dias 7 e 8 de abril de 2016.

* Professora da Faculdade de Direito da Universidade de Lisboa.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3.

Prova digital: enquadramento legal

João Conde Correia

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3. PROVA DIGITAL: ENQUADRAMENTO LEGAL[1]

João Conde Correia*

Antes de começar propriamente permitam-me ainda que vos conte uma pequena história.

Há pouco tempo, num encontro internacional de magistrados, um velho conhecido, juiz num país do norte da Europa, perguntou-me como estava regulada a prova digital em Portugal.

Respondi-lhe que formalmente a prova digital estava regulada:

– No CPP;

– Na Lei 32/2008, de 17/07;

– Na Lei 109/2009, de 15/09.

Ele escutou-me com muita atenção e depois disse que, com três leis, o nosso sistema devia ser muito bom e que certamente não teríamos problemas práticos, como aqueles que se suscitam no seu país.

Nessa altura, pensando melhor, tive que lhe dizer que a quantidade nem sempre é sinónimo de qualidade e que também entre nós há muitos problemas teóricos e práticos.

De facto, a teia legislativa nacional é muito complexa, sobrepondo-se em camadas sucessivas, que ora parecem divergir e ganhar autonomia, ora parecem convergir e superar-se sucessivamente, tornando quase impossível a tarefa do melhor intérprete.

As peças do *puzzle* não se encaixam facilmente.

Em vez de seguir o velho conselho iluminista e de optar por poucas leis, simples e claras o *legislador* escolheu a via incerta da pluralidade e da complexidade, gerando um sistema anárquico, onde, muitas vezes, nem a letra, nem o seu espírito, nem, tão pouco, a sua história fornecem a bússola necessária para encontrar o caminho mais seguro.

Por isso mesmo, parafraseando Alexander Graf zu Dohna: a jurisprudência dificilmente conseguirá resolver a quadratura do círculo ou desatar os apertados nós que o legislador foi atando.

*

[1] O texto corresponde às notas que serviram de apoio à intervenção do autor na ação de formação "Prova em Direito Penal, cibercriminalidade e prova em ambiente digital", no CEJ, nos dias 7 e 8 de abril de 2016.
*Procurador da República.

Uma simples leitura formal do CPP revela um primeiro nó.

O *legislador*, misturando realidades técnicas muito diferentes, estende, ainda hoje, o regime previsto para as interceções telefónicas, a outras conversações ou comunicações, transferidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital (artigo 189.º, n.º 1).

Para além disso, regula, igualmente, a obtenção e junção aos autos de dados sobre a localização celular ou de registos de realização de conversações ou comunicações (artigo 189.º, n.º 2).

A interpretação desta norma, já denominada «'casa dos horrores' hermenêuticos» não é simples nem linear.

Ao aglutinar diversas realidades, carecidas de graus de tutela diversos e de distintas exigências práticas, o legislador deu um contributo decisivo para a incerteza e para a insegurança jurídicas e dificultou a tarefa das instâncias formais de controlo.

Com efeito, na parte em que estende o regime das escutas telefónicas ao *e.mail* guardado no computador do destinatário, o preceito veio dificultar desmesuradamente a investigação criminal, assegurando a estes documentos uma tutela mais consistente do que a oferecida pelo regime das *buscas*. Regime a que, em primeiro, deviam ser submetidas as intromissões nestes documentos.

Para além disso, a desconsideração dos interesses da investigação era, ainda, visível na impossibilidade de intercetar as comunicações eletrónicas ou sequer de obter os respetivos dados de tráfego, no caso de crimes informáticos ou de injúria, ameaça, coação ou devassa da vida privada cometidos por via informática.

Devido àquela cláusula de extensão (artigo 189.º), estes crimes também não beneficiavam destes meios, excepcionais, de investigação.

O legislador esqueceu assim as situações em que, paradoxalmente a intromissão é mais necessária e legítima, tornando quase impossível investigar estes crimes com sucesso.

*

Pouco tempo depois, agravando as grandes dificuldades interpretativas geradas sobretudo pela alteração do CPP, a Lei n.º 32/2008, de 17/07, resultante de uma Diretiva Europeia (2006/24), veio também regular a conservação e a transmissão dos dados de tráfego e de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador registado para fins de investigação destes e repressão de crimes graves.

Nos termos desta Lei, a transmissão destes dados só é admissível:

– Num catálogo restritivo de crimes;

– Por despacho fundamentado do JIC;

– Quando houver razões para crer que são indispensáveis para a descoberta da verdade ou para a prova daqueles e que esta será de outra forma impossível ou muito difícil de obter; e

– Deve respeitar os princípios da adequação, necessidade e proporcionalidade (artigo 9.º, n.ºs 1 e 2).

Para além disso só podem ser transmitidos dados relativos:

– Ao suspeito ou arguido,

– À pessoa suspeita de receber ou transmitir mensagens destinadas ou provenientes daqueles ou, mediante consentimento, à própria vítima (artigo 9.º, n.º 3).

Desta forma, apesar de convocar requisitos de acesso semelhantes, o legislador, sem qualquer razão técnica válida, duplicou os regimes, consagrando normas gerais no CPP e normas especiais na Lei n.º 32/2008.

*

Por último, a Lei n.º 109/2009, apesar da sua denominação equívoca e aparentemente restritiva (LC), veio acrescentar mais um apertado e desnecessário nó górdio.

Na verdade, as disposições processuais penais nela contidas aplicam-se:

– Aos crimes aí previstos (C. informáticos *stricto sensu*);

– Aos crimes cometidos por meio de um sistema informático e, ainda,

– Aos crimes em que seja necessário proceder à recolha de prova em suporte eletrónico (artigo 11.º, n.º 1), assumindo uma vocação transversal a todo o sistema processual penal.

Podemos mesmo dizer que, em matéria de prova, constitui, agora, a sua pedra angular.

De facto, passaram a reger-se por esta nova lei especial:

– A pesquisa de dados informáticos (artigo 15.º);

– A apreensão de dados informáticos (artigo 16.º);

– A apreensão de correio eletrónico e de registos de comunicações de natureza semelhante (artigo 17.º); e

– A interceção de comunicações (artigo 18.º).

Com a publicação desta nova lei, satisfazendo as obrigações internacionais do Estado Português, o legislador nacional consagrou, finalmente, um verdadeiro sistema processual de prova digital.

Todavia, mais uma vez, a opção legislativa passou pela escolha da via lateral e acessória da legislação extravagante, em detrimento do aconselhável regime geral.

Em vez de uma, as fontes da prova digital passaram, entre nós, a ser três...

*

A coexistência formal destas três normas gera extensas zonas de confronto e de atrito, porventura impercetíveis ao observador menos atento.

O *puzzle*, repito, não se conjuga facilmente.

Na *praxis* jurídica quotidiana continuam a existir abundantes exemplos da falta de articulação destas três normas.

Do ponto de vista doutrinal parece claro, desde logo, que a Lei 32/2008 e, depois, a Lei 109/2009 revogaram tacitamente parcelas importantes do regime consagrado no artigo 189.º do CPP, reduzindo muito o seu alargado âmbito de aplicação inicial.

Estas leis extravagantes sobrepõem-se àquele regime geral, que só subsiste naquilo que não foi depois especialmente regulado.

Já as relações entre a Lei n.º 32/2008 e a Lei n.º 109/2009 são mais complexas.

Segundo a tese minoritária a LC. revogou o regime de acesso àqueles dados subsistindo a Lei n.º 32/2007, sobretudo no que concerne ao «estabelecimento dos deveres dos fornecedores de serviços e prestação desses dados».

Este seria, afinal, o sentido útil da ressalva do legislador.

Aquela lei só sobrevive naquilo que não foi expressamente regulado pela LC. Não há nenhuma razão para manter regimes diversificados de acesso e que, contraditoriamente, oneram a investigação dos crimes mais graves com exigências injustificadas.

Em sentido contrário, a tese maioritária advoga que relação será antes de pura complementaridade.

O próprio legislador afirmou-o solenemente na LC (artigo 11.º, n.º 2).

Assim, restaria ao intérprete o pesado ónus de determinar os respetivos âmbitos de aplicação, delimitando campos que parecem sobrepostos, mas são afinal contíguos.

A guarda e conservação dos dados de tráfego e de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador registado para fins de investigação destes e repressão de crimes graves, independentemente de um qualquer pedido das autoridades oficiais e, mesmo, de uma qualquer suspeita da prática de um crime, justificará maior dificuldade e cuidado no acesso a essa informação.

Quanto maior for o acervo de informação sensível existente, maior deverá ser o cuidado no seu acesso.

Já que o legislador impõe a conservação preventiva destes dados, ao menos que restrinja a possibilidade da sua utilização apenas aos casos que um juiz considere indispensáveis.

*

Este relacionamento difícil (seja ele qual for) foi, recentemente, abalado pela declaração de invalidade da Diretiva n.º 2006/24/EU do PE e do Conselho de 15/03/2006, tornando a convivência mais difícil ou, mesmo, impossível.

Segundo o TJUE (8/04/2014), a obrigação de conservar aqueles dados e a possibilidade de aceder a eles interfere de forma desproporcionada com os Direitos Fundamentais ao respeito pela vida privada e à proteção dos dados pessoais:

> – Os contornos da restrição daqueles direitos não estão suficientemente circunscritos, não garantindo que ela se limita ao estritamente necessário;
>
> – Não foram estabelecidas diferenciações objetivas e subjetivas;
>
> – Nada garante que o acesso aos dados se limite à prevenção e repressão de crimes graves;
>
> – O período de retenção não foi criteriosamente definido e os riscos de abuso limitados.

Por isso foi declarada inválida.

Mas sobre tudo isto irá falar-vos o Doutor David Silva Ramalho.

*

Ademais destes problemas formais, resultantes de uma técnica legislativa desadequada, também as próprias soluções legais suscitam algumas reservas materiais.

É que a escolha nem sempre foi a mais correta.

Nuns casos foram claramente esquecidas as exigências de uma ação penal eficaz, como novo e autónomo bem jurídico, constitucionalmente reconhecido e sancionado.

Noutros é a proteção dos direitos individuais, enquanto inquestionável finalidade primária do próprio processo penal, que ficou demasiado fragilizada.

O legislador ainda não atingiu o ponto ideal da concordância prática dos interesses conflituantes, sempre inerentes ao processo penal de um Estado de Direito.

Um dos pontos mais discutíveis (e carecidos de reforma) do regime legal da prova digital consiste na tutela processual penal conferida ao correio eletrónico já recebido.

À semelhança do correio tradicional também ele deveria ser tratado como um simples documento.

Depois de recebido, lido e guardado no computador do destinatário, o *e-mail* deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito.

E, como tal sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado.

Podendo, como tal, figurar como objeto idóneo da *busca* em sentido tradicional.

No entanto, malgrado a bondade desta doutrina e a autoridade científica dos seus defensores, o legislador não foi muito claro, deixando espaço suficiente para a polémica desnecessária e inútil.

Numa perspetiva literal, não tendo ele estabelecido qualquer distinção legal, também o intérprete não deverá separar, beneficiando o correio aberto e lido do regime previsto para todo o restante.

Em ambos os casos só a autorização judicial legitima a sua apreensão.

O legislador terá querido conferir uma tutela ao correio eletrónico armazenado superior à conferida aos vulgares escritos.

No fundo «um *plus* de proteção a arquivos que já foram comunicação, em nome da salvaguarda da privacidade da autodeterminação informacional».

Uma leitura integrada e coerente, que acentue as inevitáveis semelhanças com os escritos tradicionais e as suas necessidades de tutela, tenderá, todavia, a excluir este correio, considerando-o como um mero documento e facilitando a sua apreensão: será suficiente a intervenção do magistrado do Ministério Público, nos termos do artigo 16.º da Lei n.º 109/2009.

À semelhança de uma carta recebida, também o correio eletrónico aberto deverá poder ser, por ele, apreendido.

Só assim fará, aliás, sentido convocar as normas relativas à apreensão de correspondência para a obtenção das restantes comunicações (artigo 17.º).

*

Outra incongruência do legislador consiste na aparente impossibilidade formal de realizar interceções de comunicações, ou sequer de obter os respetivos dados de tráfego, para prova dos crimes previstos na LC ou de injúrias, de ameaças, de coação, de devassa da vida privada cometidos por meio de CE.

Nos termos do artigo 18.º da LC a intercepção das comunicações só é aqui admissível quando os crimes se encontrem previstos no artigo 187.º do CPP.

Uma leitura literal tenderá, portanto, a excluir todos os outros crimes.

Esta tese, que parte da manutenção formal do famigerado artigo 189.º do CPP, é inadmissível:

> 1.º Porque nos casos previstos no artigo 18, n,º 1, a) a interceção não depende de qualquer outro requisito adicional, *maxime* da respetiva moldura penal abstrata (foi, por isso mesmo, que o legislador autonomizou as duas alíneas do referido artigo, ainda que os requisitos adicionais, previstos na alínea b), só se aplicam aos casos aí referidos);
>
> 2.º Porque a remissão para o catálogo de crimes constante do artigo 189.º do CPP deverá, numa interpretação atualista, incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos através de sistema informático.

O propósito do legislador, embora muito mal expresso, foi, justamente, permitir a «realização de interceção de comunicações eletrónicas e, sobretudo a obtenção de dados de tráfego» nos «processos crimes em que se investiguem crimes cometidos por via das redes de comunicações».

A remissão legal é, assim, para o tipo de crime e não para a forma como ele é cometido, pois essa passa necessariamente por um sistema informático, como resulta da primeira parte da alínea b) do n.º 1 do artigo 18.º («cometidos por meio de um sistema informático»).

O que ali é autorizado para os crimes praticados através do telefone é aqui permitido para os crimes cometidos através de um sistema informático.

Na verdade, não podemos esquecer que a CRP não prevê formas de utilização abusiva deste direito.

O sigilo das comunicações não foi concedido para, a seu coberto, se poder insultar, ameaçar ou coagir outrem ou para se poder devassar a sua vida privada.

Nestes casos, apesar da sua reduzida relevância penal, o Estado deve ter legitimidade para intervir. Nada justifica, por isso, destacar as ofensas cometidas por telefone, conferindo-lhes uma tutela processual penal muito superior às restantes.

*

As soluções do nosso legislador parecem ter ignorado, igualmente, as potencialidades da chamada comunicação entre máquinas ou, pelo menos, silenciada uma opção clara, que evitasse o improviso, o casuísmo e a consequente insegurança jurídica.

A fronteira entre dados de tráfego (artigo 2.º, alínea c), relativos a comunicações realizadas ou falhadas e, logo, sujeitos a uma maior reserva e os restantes dados de comunicação (artigo 14.º), que não pressupõem uma qualquer intervenção humana não é nítida e inequívoca.

Nem todas as informações disponibilizadas pelos aparelhos de telecomunicações beneficiam do seu sigilo.

A simples comunicação entre máquinas não está aqui incluída.

Na clara formulação do BverfG: «uma comunicação técnica entre aparelhos não apresenta o específico potencial de perigo garantido pela proteção do artigo 10.º, § 1.º, da Lei Fundamental.

A identificação do INSI ou do IMEI não realiza o específico perigo para a privacidade provocado pela utilização de um meio de comunicação.

Por isso mesmo, estes dados não estão protegidos pela garantia da inviolabilidade das telecomunicações.

Não há aqui nenhuma troca de informação, provocada por um ser humano, relativa ao conteúdo de uma comunicação.

A sua transmissão ocorre independentemente de uma qualquer comunicação ou sequer ligação, destinando-se, apenas, a assegurar a capacidade de resposta do operador, no caso de ser efetivamente utilizado.

Os dados de tráfego só incluem, portanto, o registo de impulsos comunicativos, ainda que falhados, desencadeados por humanos.

De fora ficam «os procedimentos de identificação do número de um aparelho de telemóvel ou do respetivo cartão (*IMEI e IMSI*).

O mesmo valendo para os consequentes dados obtidos, concretamente os dados de localização logrados através destes procedimentos».

Tratamento semelhante devem ter aquelas situações em que ainda não está em causa a identificação de uma pessoa, mas apenas uma máquina ou a sua localização.

*

Um dos exemplos mais flagrantes das dificuldades de conjugação entre o regime especial (LC) e o regime geral (CPP) consiste na articulação entre a pesquisa de dados informáticos (artigo 15.º da Lei n.º 109/2009, de 15 de setembro) e as perícias (artigos 151.º e ss. do CPP) e os exames (artigos. 171.º do CPP).

A relação entre estes três instrumentos processuais penais também não é muito clara.

A opção por um regime especial poderá, desde logo, fazer supor que a pesquisa de dados informáticos (artigo 15.º) se sobrepõe, incondicionalmente, ao regime geral dos meios de prova e de obtenção da prova, consagrado no CPP, *maxime* à prova pericial (artigos 151.º e ss.) e aos exames (171.º e ss.).

A única forma de aceder ao conteúdo de um computador seria a pesquisa de dados informáticos, sendo todas as outras ilegítimas.

O artigo 11.º da Lei n.º 109/2009, para além de determinar, pela via positiva, o âmbito de aplicação processual das suas disposições, excluiria, pela via negativa, a aplicação de qualquer outra lei.

Esta visão, redutora e superficial, não corresponde, de forma alguma, à realidade.

A pesquisa informática (que no fundo não é mais do que uma busca realizada num computador) tem pressupostos e objetivos claramente determinados e circunscritos (obtenção de dados informáticos específicos e determinados, armazenados num computador) que não prejudicam o regime geral.

Em certas circunstâncias poderá, por exemplo, ser necessário proceder a uma perícia informática ou até, mesmo, examinar um computador.

Aliás, a própria Lei do Cibercrime fala de «pesquisa informática ou de outro acesso legítimo a um sistema informático» (artigos. 16.º e 17.º) demonstrando que, afinal, aquela lei não detém o exclusivo na aquisição processual de dados informáticos.

O legislador reconheceu a existência de outras formas, retornando assim ao CPP, que *ab initio* quis afastar.

*

Noutro quadrante axiológico, interferindo agora com o desejável nível de proteção dos Direitos Fundamentais, surge o consentimento para a pesquisa informática de quem tenha disponibilidade ou controlo sobre esses dados (artigo 15.º, n.º 3) e não do acordo prévio do próprio visado (artigo 174.º, n.º 5, alª b).

Solução que facilita as funções das instâncias formais de controlo, mas desconsidera irremediávelmente a reserva da intimidade da vida privada do visado, admitindo que um terceiro possa permitir o acesso aos dados – sejam eles quais forem – ali guardados.

O computador funciona hoje, muitas vezes, como uma extensão da personalidade (substituindo, em muitos casos, os tradicionais diários), podendo conter escritos, imagens, sons ou outros registos relativos ao núcleo intangível e absoluto da intimidade de cada um, pelo que só ele deverá poder decidir se os torna ou não públicos.

Tratando-se de um computador pessoal, quem tem disponibilidade sobre ele não terá, em princípio, legitimidade para autorizar a intromissão no seu conteúdo.

Isto não significa, como é óbvio, que o computador não possa ser acedido (transformando-o numa espécie de território sagrado), mas apenas que deverá haver mais cuidado no seu acesso não legitimado por uma qualquer autorização legal válida.

O visado deverá poder exigir que o Estado apenas interfira no conteúdo do seu computador mediante o seu próprio consentimento ou, então, mediante mandado oficial.

*

Alheio à discussão sobre a autoridade competente para determinar a apreensão do correio eletrónico lido é, ainda, o caso semelhante das comunicações voluntariamente disponibilizadas pelo seu recetor.

A Jurisprudência Penal tem destacado, de forma constante, que as regras relativas à apreensão não se aplicam quando os dados pretendidos são «espontaneamente fornecidos por quem pode dispor deles livremente.

À semelhança da entrega de uma carta recebida ou da disponibilização de uma mensagem gravada no *voice mail*, também o correio eletrónico recebido está na disponibilidade do seu recetor.

Quem remete uma carta, grava uma mensagem, ou envia um *email* sabe que a partir do momento em que ela for recebida, deixa de contar com o sigilo das comunicações, ficando nas mãos do destinatário, tendo que contar com a sua eventual indiscrição.

*

Esta indesejável anarquia das fontes normativas, aliada à insolvabilidade de algumas soluções materiais, para além de testemunhar a qualidade técnica do nosso legislador atual, impõe que se reflita sobre a lei que devíamos ter.

Por um lado, porque a qualidade da lei vigente é condição essencial para a qualidade do direito quotidianamente aplicado.

Por outro lado, porque o constante progresso científico reclama uma atuação constante do legislador.

É necessário que ele adeqúe o direito processual penal às novas realidades disponibilizadas pelo contínuo progresso científico e logo utilizadas pela criminalidade.

O simples facto de estarem disponíveis não significa que sejam legítimos e admissíveis, carecendo de mediação legal expressa, que transforme a possibilidade em realidade jurídica.

Entre os fatores que mais têm contribuído para a insegurança jurídica e consequente acentuar da crise da justiça destacam-se a instabilidade, a complexidade, a confusão e a inflação legislativa, que atingem níveis nunca antes alcançados.

As leis contam-se, em todos os países, pelas dezenas de milhar, de tal forma que os nossos ordenamentos regrediram à incerteza e à arbitrariedade que caracterizaram «o direito jurisdicional pré-moderno».

Por todo o lado surgem normas processuais penais especiais, muitas vezes difíceis de compatibilizar com o regime geral: vai-se instalando «a desordem e a insegurança jurídicas, coincidentes com uma profunda crise dos nossos valores comunitários e expressão de reflorescentes concepções do mundo, turvas e regressivas».

O CPP, apesar da sua juventude e da sua notável capacidade de adaptação e de evolução, enfrenta, há muito, as sérias tensões centrípetas da desordem e da descodificação profundas.

As Leis n.ºs 32/2008 e n.º 109/2009 são mais um triste exemplo desta nova abordagem, que privilegia o particular em detrimento do global.

Por não ter a coragem política necessária ou, então, o engenho suficiente para, mais uma vez, alterar o CPP, o legislador – invocando uma má tradição – enveredou pela via lateral.

Aquilo que constitui hoje o cerne da prova foi remetido para a lei secundária.

Urge, por isso, recuperar a centralidade normativa do CPP, enquanto instrumento nevrálgico da perseguição criminal, reservando para a legislação especial aquilo que é acessório, técnico, excecional. Normas como as que preveem a prova digital, pela sua importância, pelos interesses que regulam, pelas consequências que desencadeiam e, até, pela frequência com que são utilizadas devem constar do CPP.

*

Para além de utilizar técnicas legislativas de duvidosa legitimidade teórica e de nula eficácia prática e de nem sempre escolher as melhores soluções materiais, o legislador – mesmo quando advertido pelas vozes mais autorizadas da ágora nacional – persiste em incompreensíveis omissões legislativas, criando lacunas inadmissíveis.

Como já vimos, alguns dos nódulos mais problemáticos continuam por regular.

Para além disso, o progresso científico vem criando novos problemas.

Aquilo que há poucos dias era fixação surge hoje como a mais banal das realidades.

Seja qual for a solução técnica adotada impõe-se, portanto, a atualização urgente da malha legislativa nacional, por forma a superar essas lacunas e a corrigir os estrangulamentos resultantes da incoerência de algumas soluções legais.

*

As leis que temos, malgrado a sua estranha perfusão, não resolvem, expressamente, o momentoso problema das buscas *online*.

É hoje possível, mediante várias técnicas informáticas à distância, via *internet,* aceder aos dados contidos num computador, observá-los, monitorizá-los, copiá-los sem o conhecimento ou consentimento do visado.
A garantia do sigilo das telecomunicações (artigo 34.º, n.º 4, da CRP) protege a transferência (por telefone, cabo, via analógica, digital, etc.) de dados (escritos, sons, imagens desenhos, etc.) mas não a confidencialidade ou a integridade do próprio sistema informático.

Assim, embora sejam um ato de telecomunicação, as buscas *online* não são uma intromissão nas telecomunicações.

Em causa estará, quando muito, «a integridade e confidencialidade do sistema informático» ou, então, a esfera privada digital ou eletrónica e não um qualquer ato de comunicação.

Por outro lado, em comparação com as buscas tradicionais, estes procedimentos configuram – devido à sua elevada intensidade intrusiva – uma medida com caráter novo e independente.

A realização das diligências a descoberto dá ao visado a possibilidade de, segundo as circunstâncias do caso, impedir a concretização da medida, entregando a coisa procurada, circunscrever a sua duração e intensidade e, até, com a ajuda de um advogado, controlar a existência e o respeito pelos pressupostos legais, *maxime* a decisão que a autoriza.

A sua realização secreta, pelo contrário, retira ao visado qualquer possibilidade de controlo.

Por falta de autorização legal expressa, as buscas *online* seriam assim inadmissíveis.

Mesmo assim parece haver alguma margem de constitucional para a implementação processual penal destas medidas.

Segundo o BVerfG a infiltração secreta em sistemas informáticos alheios, para efeitos de monitorização ou de leitura de dados, será constitucionalmente admissível, mediante prévia autorização judicial, em casos de perigo concreto para bens jurídicos individuais como a vida, o corpo ou a liberdade ou para interesses coletivos, cuja ameaça afete os fundamentos ou a sobrevivência do Estado de direito ou da própria existência humana.

A concretização processual penal desta estreita margem de disponibilidade constitucional deverá ser uma tarefa urgente do legislador nacional.

A luta contra as expressões mais graves da criminalidade, que ameaçam a sobrevivência do próprio Estado de Direito, deve poder contar com esta possibilidade suplementar.

O sistema processual tem que estar preparado para resolver os problemas que lhe venham a ser colocados.

*

A localização das viaturas dos suspeitos através da tecnologia GPS também não mereceu ainda a atenção do legislador nacional.

Apesar de ser uma diligência com extrema importância para a descoberta da verdade e que pode substituir as vigilâncias e seguimentos tradicionais (poupando tempo e meios) colocar um aparelho GPS na viatura dos suspeitos, sem o seu conhecimento ou consentimento, para depois determinar a sua posição e movimentos, continua sem cobertura legal expressa.

Neste contexto, um acórdão da RE decidiu que não carece de prévia autorização judicial o uso pelos OPC de localizadores de GPS colocados em veículos utilizados pelas pessoas investigadas.

Para o efeito, a RE invocou que a utilização daqueles aparelhos não consubstancia nenhum método proibido de prova (artigo 126.º), não podendo sequer «ser visto como uma violação

da vida privada de quem vai nesse veículo, pois que o GPS é um aparelho surdo e cego no sentido de que não escuta as conversas dos ocupantes do carro, nem identifica quem lá vai e o que estão a fazer, apenas informa onde está o veículo».

No fundo, só permite estabelecer a localização do aparelho emissor do sinal.

Já um acórdão da RP, defende que o uso de localizadores GPS pelos OPC e a sua monitorização «permite traçar o perfil detalhado da vida pública e privada de uma pessoa» pelo que «deve ser sujeita a autorização judicial, aplicando-se, por interpretação analógica, o artigo 187.º do CPP».

Na verdade, «não faria sentido que apenas fosse sujeita a autorização judicial a localização celular através dos dados telefónicos e já não o fosse o acesso a dados de localização através do mecanismo GPS, uma vez que se tratam de dados sensíveis, que dizem respeito à vida íntima e encontram-se no âmbito do DF à autodeterminação informativa».

Desprezar as potencialidades probatórias da localização GPS é – num mundo cada vez mais tecnológico – um absurdo jurídico em que nenhum legislador preocupado com a eficácia da justiça penal quererá incorrer.

O progresso científico não pode ser afastado do processo penal, nem remetido apenas para o livre arbítrio do julgador.

Circunscrever as hipóteses em que ele pode ocorrer é, pois, um imperativo ético jurídico de um legislador atento, preocupado com a defesa dos direitos fundamentais, mas também com a criação de condições para um efetivo exercício do *ius puniendi* estadual.

*

Outra questão que a malha legislativa nacional ainda não resolve é a da eventual revelação coativa de *passwords*.

Os OPC, O MP, ou o JIC podem ou não notificar os possuidores de computadores para entregar as suas *passwords* a fim de – rompendo o bloqueio – terem acesso ao conteúdo dos mesmos.

Apesar dos exemplos, colhidos noutros quadrantes, a solução não é linear, cruzando várias linhas centrípetas, difíceis de harmonizar.

Quando o notificado for o próprio arguido, não havendo entre nós nenhuma norma habilitante, dificilmente se poderão superar os constrangimentos processuais decorrentes do princípio *nemo tenetur se ipsum accusare*.

O arguido não pode ser forçado a contribuir para a sua própria condenação.

Ainda assim, não se tratando de um princípio absoluto, o legislador poderá criar situações circunscritas em que seja proporcional impor a colaboração do arguido, como, por exemplo, aquelas hipóteses em que, sem a *password*, determinada informação vital não possa ser obtida em tempo útil.

Quando o notificado for uma mera testemunha (situação menos provável, mas ainda possível) a solução será mais fácil.

Excecionando, os casos em que possa validamente recusar-se a prestar declarações (artigos 132.º, n.º 2 e 134.º), a recusa em fornecer a *password* será ilegítima, podendo ser sancionada.

Vídeo da apresentação

https://educast.fccn.pt/vod/clips/13vwtviahd/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4.

A Prova Digital perante a Proteção de Dados Pessoais - uma perspetiva Portuguesa e Europeia

Manuel David Masseno

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4. A PROVA DIGITAL PERANTE A PROTEÇÃO DE DADOS PESSOAIS – UMA PERSPETIVA PORTUGUESA E EUROPEIA[1]

Manuel David Masseno*

Apresentação *Power Point*
Vídeo

Apresentação *Power Point*

[1]Apresentação decorrida na ação de formação "Prova em Direito Penal, cibercriminalidade e prova em ambiente digital", no CEJ, nos dias 7 e 8 de abril de 2016.
* Professor do Instituto Politécnico de Beja.

A Prova Digital perante a Proteção de Dados Pessoais

Um *Pré-entendimento*:

- na **Sociedade em Rede**, *hoc sensu*, **o equilíbrio conflitual entre os Poderes e as Liberdades passa pela consideração da *Autodeterminação Informacional***
  - aliás, **será que hoje ainda faz sentido pensar em termos de *privacidade*, em termos negativos?**
- daí a ***constitucionalização* da Proteção de Dados**:
  - em **Portugal** (Art.º 35.º da ***Constituição da República Portuguesa***), desde **1976**
  - na **União Europeia** (Art.º 16.º do ***Tratado sobre o Funcionamento da União Europeia*** e Art.º 8.º da ***Carta dos Direitos Fundamentais da União Europeia***), a partir o ***Tratado de Lisboa***, de **2007/2009**

A Prova Digital perante a Proteção de Dados Pessoais

E um segundo… até conclusivo

- **como será óbvio**, mas nem sempre é colocado em evidência, sobretudo **num Estado de Direito**, **as questões dos fins e dos meios devem estar sempre presentes no combate ao crime**
- *id est*, **as ações de prevenção, de investigação criminal e também a atuação dos tribunais apenas estão legitimadas se tiverem como finalidade e decorrerem no** estrito **quadro dos Direitos Fundamentais, de todos**, incluindo os investigados e os arguidos, **tendo por referência constante o *Princípio da Proporcionalidade***
- por outras palavras, **não é sequer concebível um *Direito Penal do Inimigo*…** mesmo se *Terrorista*

3

Sumário:

I. A Constitucionalização dos Direitos Fundamentais também pela União Europeia

II. A Autodeterminação Informacional e a Investigação Criminal

III. A Jurisprudência do Tribunal de Justiça da UE

I. A Constitucionalização dos Direitos Fundamentais também pela União Europeia

a) a natureza *constitucional* do Ordenamento da União:

- **desde o seu início**, nas palavras de Walter Hallstein, a **Comunidade/União Europeia é uma Comunidade de Direito** (*Rechtsgemeinschaft*), **e** o **Tribunal de Justiça** construiu um Ordenamento tendo-o em mente,
- **com o *Tratado de Lisboa*, um tal papel ficou ainda mais explícito:** "A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem" (Art.º 2.º do *Tratado da União Europeia*)

A Prova Digital perante a Proteção de Dados Pessoais

- antes de mais, **temos o Princípio do Primado do Direito da União sobre os Direitos Nacionais:**
  - **enunciado no Acórdão** de 15 de julho de **1964** (C-6/64), **Costa/ENEL**
  - **reiterado no Acórdão** de 9 de março de **1978** (C-106/77), **Simmenthal, e no Acórdão** de 19 de junho de **1990** (C-213/89), **Factortame**
- a partir do Princípio da Lealdade, o Tribunal de Justiça construiu o **Princípio da Interpretação Conforme ao Direito da União**, ou Aplicabilidade Indireta
  - **com os Acórdãos** de 10 de Abril de **1984** (C-14/83), **von Colson e Kamann,** de 4 de fevereiro de **1988** (C-157/86), **Murphy, e** de 13 de novembro de **1990** (C-106/89), **Marleasing**

6

A Prova Digital perante a Proteção de Dados Pessoais

- mas, **com as reservas,** sobretudo em matéria penal, **constantes dos Acórdãos** de 11 de junho de **1987** (C-14/86), **Pretura di Salò**, de 8 de outubro de **1987** (C-80/86), **Kolpinghuis Nijmegen**, de 26 de setembro de **1996** (C-168/95), **Arcaro**, **e** de 4 de julho de **2006** (C-212/04), **Adeneler**
- **Princípios estes que integram o *acquis* e foram recebidos pela *Constituição da República*, "**As disposições dos tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respetivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático.**"** (Art.º 8.º n.º 4)

7

A Prova Digital perante a Proteção de Dados Pessoais

- de onde resulta que **os Juízes nacionais são também Juízes da União**, mesmo quando aplicam normas de Direito interno não resultantes da transposição de Diretivas, *maxime* quando aos regimes comunitários que estão em vias de vigorar:
  - *v.g.*, **a** nova **Diretiva 2016/343**, do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativa ao **reforço de certos aspetos da presunção de inocência e do direito de comparecer em julgamento em processo penal ou**
  - **a** novíssima **Diretiva 2016/680** do Parlamento Europeu e do Conselho, 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 ou execução de sanções penais**, e à livre circulação desses dados

8

A Prova Digital perante a Proteção de Dados Pessoais

II. A Autodeterminação Informacional e a Investigação Criminal

a) no que se refere à Proteção de Dados Pessoais

- assim, **na União Europeia, "1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.**

  2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes." (Art.º 16.º do *TFUE*)

9

A Prova Digital perante a Proteção de Dados Pessoais

- **e na *Carta dos Direitos Fundamentais da União Europeia***
  - "1. **Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito**.
    2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada [titular dos dados] ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
    3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." (Art.º 8.º)
    - **recordando que "A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia**, de 7 de Dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, **e que tem o mesmo valor jurídico que os Tratados."** (Art.º 6.º do ***TUE***)

10

A Prova Digital perante a Proteção de Dados Pessoais

- **no que se refere ao Direito derivado, temos um *microssistema* centrado na Diretiva 95/46/CE**, do Parlamento Europeu e do Conselho, de 24 de outubro de **1995**, relativa **à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais** e à livre circulação desses dados**, completado pela**
  - **a Diretiva 2002/58/CE**, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao **tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas**
  - **o Regulamento n.º 45/2001**, do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à **proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados e**
  - **a Decisão-Quadro 2008/977/JAI**, do Conselho, de 27 de novembro de 2008, relativa à **proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal**

11

A Prova Digital perante a Proteção de Dados Pessoais

- cumpre referir **ainda o novo** Regulamento 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (**Regulamento Geral sobre a Proteção de Dados**)
- **a Diretiva 2016/680** do Parlamento Europeu e do Conselho, 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 ou execução de sanções penais**, e à livre circulação desses dados **e ainda**
- **a Diretiva 2016/681** do Parlamento Europeu e do Conselho, relativa à **utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave**
  - todos de 27 de abril, publicados a 4 de maio de 2016.

12

A Prova Digital perante a Proteção de Dados Pessoais

- **em Portugal**, desde 1976, **a Lei Fundamental dispõe**, incorporando o devir das Fontes europeias:
  - **"1.** Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei**.**

    2. A lei define o conceito de dados pessoais, bemcomo as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

    [...]

    4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei." (Art.º 35.º - Utilização da informática)

13

A Prova Digital perante a Proteção de Dados Pessoais

- **e nas Leis ordinárias**:
  - **a Lei n.º 67/98**, de 26 de outubro, aprova a ***Lei da Proteção de Dados Pessoais***
  - **a Lei n.º 41/2004**, de 18 de agosto, relativa ao **tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas**, alterada pela Lei n.º 46/2012, de 29 de agosto
  - **a Lei n.º 34/2009**, de 14 de julho, estabelece o **regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial**
  - **a Lei n.º 37/2015**, de 5 de maio, estabelece os **princípios gerais que regem a organização e o funcionamento da identificação criminal**
  - **a Lei 32/2008**, de 17 de julho, relativa à **conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações**
  - **e** ainda **a Lei 109/2009**, de 15 de setembro, a ***Lei do Cibercrime***

14

A Prova Digital perante a Proteção de Dados Pessoais

b) até ao ***Tratado de Lisboa***, **a matéria Penal estava no âmbito do *Terceiro Pilar* da União**, de natureza intergovernamental, **o que a permitia apenas adotar Decisões-Quadro** (previstas pelo Art.º 34º, n.º 2, alínea b), e baseadas nos Artigos 29º, 30º, n.º 1, alínea a) e 31º, n.º 1, alínea e) do *TUE*, na versão anterior)

- apesar da Diretiva 2008/99/CE, do Parlamento Europeu e do Conselho, de 19 de novembro de **2008**, relativa à **proteção do ambiente através do direito penal e do**, correspondente, **Acórdão** do TJUE, de 13 de setembro de **2005** (Processo C-176/03), Comissão c. Conselho

- **agora, "1.** O Parlamento Europeu e o Conselho, por meio de **diretivas** adotadas de acordo com o processo legislativo ordinário, podem estabelecer **regras mínimas relativas à definição das infrações penais e das sanções em domínios de criminalidade particularmente grave com dimensão transfronteiriça** que resulte da natureza ou das incidências dessas infrações, ou ainda da especial necessidade de as combater, assente em bases comuns.

15

A Prova Digital perante a Proteção de Dados Pessoais

- 2. São os seguintes os domínios de criminalidade em causa: terrorismo, tráfico de seres humanos e exploração sexual de mulheres e crianças, tráfico de droga e de armas, branqueamento de capitais, corrupção, contrafação de meios de pagamento, criminalidade informática e criminalidade organizada." (Art.º 83º)

- ainda a **Comissão Barroso**, elaborou a **Comunicação**, **"Rumo a uma política da UE em matéria penal: assegurar o recurso ao direito penal para uma aplicação efetiva das políticas da UE"** (COM(2011) 573 final), de 20 de setembro de **2011**:
  - **"O Tratado de Lisboa dá-nos os instrumentos para enfrentar os desafios do direito penal de forma equilibrada, à luz dos direitos fundamentais da liberdade e da segurança. O novo Tratado estabelece também limites e controlos claros: nada poderá ser decidido sem o controlo democrático pleno do Parlamento Europeu e a supervisão dos parlamentos nacionais, que têm uma voz importante no processo de decisão"** (**Viviane Reading**, Vice-Presidente da Comissão Europeia)

16

A Prova Digital perante a Proteção de Dados Pessoais

Sendo **reafirmados** os, seguintes, **Princípios fundamentais:**

- "O direito penal deve manter-se sempre uma medida de **último recurso**;
- As sanções penais são reservadas **aos ilícitos graves**;
- As **medidas de direito penal podem afetar os direitos fundamentais**, pelo que **a nova legislação deve respeitar plenamente os direitos fundamentais previstos na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia de Proteção dos Direitos do Homem**;
- Todas as decisões quanto ao tipo de medida ou sanção penal a adotar devem ser acompanhadas de provas factuais claras e **respeitar os princípios da subsidiariedade** e da **proporcionalidade**."

A Prova Digital perante a Proteção de Dados Pessoais

- por seu turno, **na "*Agenda Europeia para a Segurança*"**(COM(**2015**) 185 final), de 28 de abril de 2015, **é explícita na sua ligação à opção essencial do *Tratado da União Europeia*** (Art.ºs 2 e 3.º n.º 2)**:**
  - **é colocada a tónica no respeito pelos Valores inerentes a Sociedades Abertas**, nomeadamente ao ***Princípio do Estado de Direito*** **e aos Direitos enunciados na *Carta* da União Europeia**
  - **limitando as restrições aos critérios de necessidade e proporcionalidade**, enunciados na própria ***Carta***, **e incluindo as devidas garantias de controle jurisdicional** (Art.º 52.º n.º 1) **e ainda**
  - são feitas **referências** expressas **ao *leading case*, Acórdão Digital Rights Ireland** e Seitlinger.

18

A Prova Digital perante a Proteção de Dados Pessoais

III. A Jurisprudência do Tribunal de Justiça da EU

- **em matéria relacionada com o acesso à prova digital** e antes de mais, **temos o Acórdão** de 29 de janeiro de **2008** (C-275/06), **Promusicae**:
  - **"**[…] o direito comunitário exige que os referidos Estados, na transposição dessas diretivas, zelem por que seja seguida uma interpretação das mesmas que permita **assegurar o justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária**. Seguidamente, na execução das medidas de transposição dessas diretivas, compete às autoridades e aos órgãos jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com essas mesmas diretivas mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o **princípio da proporcionalidade."**

19

A Prova Digital perante a Proteção de Dados Pessoais

- **mas**, sobretudo, **releva o Acórdão** de 8 de abril de **2014** (C-293/12 e C-594/12), **Digital Rights Ireland e Seitlinger e o.**:
  - **"Estes dados** [de tráfego], considerados no seu todo, **são suscetíveis de permitir tirar conclusões muito precisas relativamente à vida privada das pessoas cujos dados foram conservados**, como os hábitos da vida quotidiana, os locais em que se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados."
  - **assim, a ingerência nos direitos fundamentais** garantidos pelos Art.ºs 7.º (Respeito pela vida privada e familiar) e 8.º (Proteção de dados pessoais) da ***Carta***, **"[…] é de grande amplitude e deve ser considerada particularmente grave** […]

20

A Prova Digital perante a Proteção de Dados Pessoais

- **[e]** Além disso, o facto de a conservação e a utilização posterior dos dados serem efetuadas sem que o assinante ou o utilizador registado disso sejam informados **é suscetível de gerar no espírito das pessoas abrangidas**, como salientou o advogado-geral nos n.ºs 52 e 72 das suas conclusões, **o sentimento de que a sua vida privada é objeto de vigilância constante."**
- **logo**, para o Tribunal, **essencial é "analisar a proporcionalidade da ingerência observada". Até porque, "No caso vertente,** tendo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito pela vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito […], **o poder de apreciação do legislador da União é reduzido, havendo que proceder a uma fiscalização estrita."**

21

A Prova Digital perante a Proteção de Dados Pessoais

- **e ainda, "No que respeita ao caráter necessário da conservação dos dados** […], **cabe observar que é verdade que a luta contra a criminalidade grave** […] **assume primordial importância para garantir a segurança pública e a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação.** […] **No entanto, tal objetivo de interesse geral**, por mais fundamental que seja, **não pode**, por si só, **justificar que uma medida de conservação** […] **seja considerada necessária para efeitos da referida luta."…**
- **"Impõe-se pois concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais** [os previstos nos Art.ºs 7.º e 8.º da ***Carta***] **de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que a mesma se limita efetivamente ao estritamente necessário."**

22

A Prova Digital perante a Proteção de Dados Pessoais

- **na mesma linha, no Acórdão** de 6 de outubro de **2015** (C-362/14), **Schrems**, **o Tribunal reitera que:**
  - "No que respeita ao nível de proteção das liberdades e direitos fundamentais garantido dentro da União, **uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve**, segundo a jurisprudência constante do Tribunal de Justiça, **estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados**. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais sejam sujeitos a tratamento automático e exista um risco significativo de acesso ilícito aos mesmos."

23

A Prova Digital perante a Proteção de Dados Pessoais

- no que se refere a **Portugal**, a **Lei n.º 32/2008**, de 17 de Julho, relativa à **conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações**, **procedeu a uma transposição razoável**
  - na **definição de "crimes graves"** (Art.º 2.º n.º 2 alínea g), nos **prazos de conservação** (Art.º 6.º) **e** nas **garantias processuais** (Art.º 9.º)
  - **pelo que nem se colocará a questão da sua invalidade, já que os padrões constitucionais foram observados** (Art.ºs 18.º n.º 2, 34.º n.º 4 e 35.º n.º 2 da CRP)
  - adicionalmente, **esta orientação foi mantida na *Lei do Cibercrime*** (Art.º 11.º n.º 2), apesar duma controvérsia sem sentido…
  - neste domínio, cabe ainda ter em **atenção os desenvolvimentos** do Processo **Davis** (C-698/15)

A Prova Digital perante a Proteção de Dados Pessoais

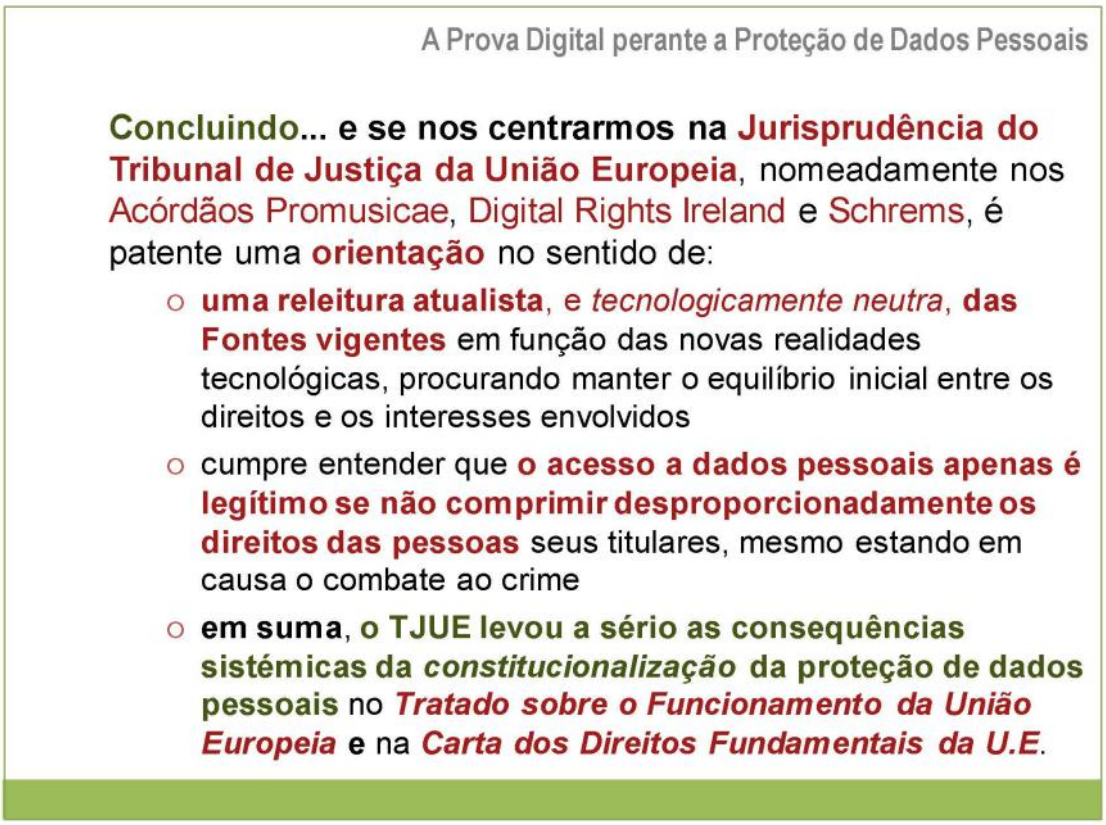
- **nesta matéria, *nossa Jurisprudência* passou por "fases":**
  - primeiro de ***desvalorização***:
    - assim, o **Acórdão da Relação de Lisboa**, de 9 de janeiro de **2002**, sobre o crime de devassa por meio da informática
  - depois de **equiparação**:
    - nomeadamente, o **Acórdão da Relação de Guimarães**, de 10 de janeiro de **2005**, sobre a violação do segredo nas telecomunicações
  - finalmente de ***consolidação***:
    - com o **Acórdão da Relação de Coimbra**, de 28 de janeiro de **2010**, sobre a identificação do utilizador nas telecomunicações telefónicas
    - o **Acórdão da Relação de Coimbra**, de 6 de abril de **2011**, sobre o crime de burla informática e a obtenção de prova **ou ainda**
    - o **Acórdão da Relação de Évora**, de 13 de novembro de **2012**, sobre difamação através da Internet e acesso aos dados do tráfego

A Prova Digital perante a Proteção de Dados Pessoais

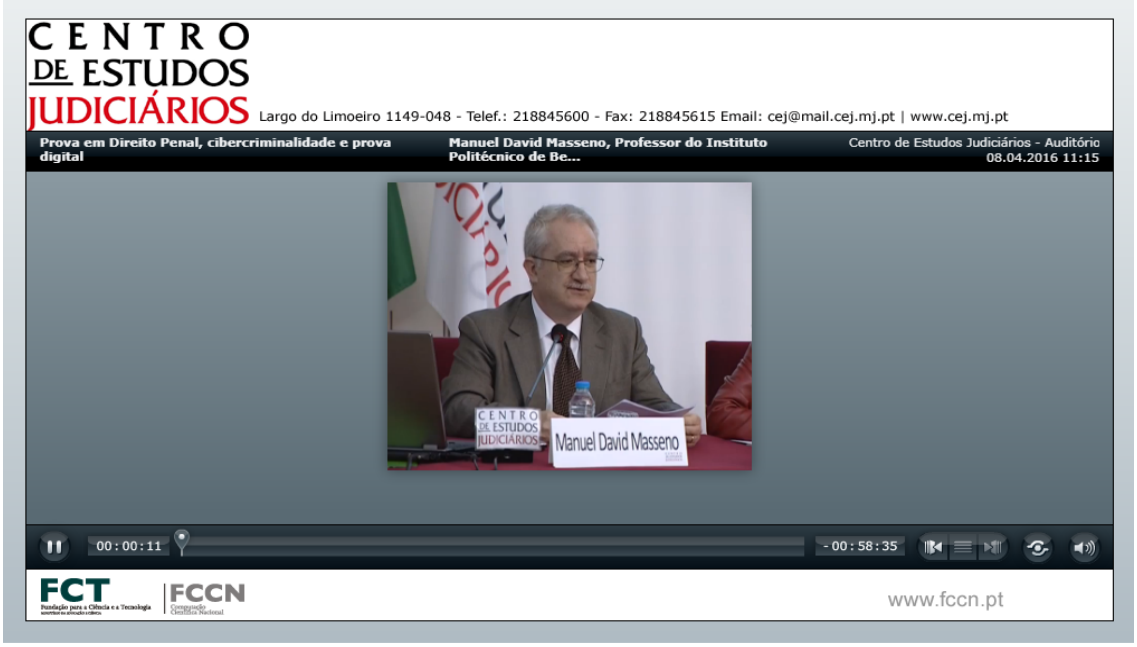
- **noutros caso, é patente o desconhecimento do conteúdo das Leis nacionais que procederam à transposição de Diretivas…** aplicando o ***Código de Processo Penal***
  - *v.g.*, o **Acórdão da Relação de Évora**, de 7 de abril de **2015**, o qual concluiu que **"encontrando-se apreendido nos autos o telemóvel em causa e o cartão SIM, ao mesmo associado, o exame pericial aos mesmos, relativo à respetiva lista telefónica, aos registos das chamadas recebidas e atendidas, das recebidas e não atendidas e, das chamadas efetuadas, não carece da prévia autorização do Juiz de Instrução.", *esquecendo*** que, na sequência da Lei n.º 46/2012, de 29 de agosto, a qual transpôs a Diretiva 2009/136/CE, de 25 de novembro de 2009, **passou a ser vedado o acesso a todos os terminais de comunicações eletrónicas, sem consentimento do utilizador** (Art.º 5.º n.º 1)

A Prova Digital perante a Proteção de Dados Pessoais

- **agora** e de imediato, **terá de atender ao Regulamento Geral**, apesar deste só entrar em vigor a partir de 25 de maio de 2018 (Art.º 99.º n.º 2), **o mesmo para a nova Diretiva sobre proteção de dados em matéria penal**, a ser transposta até 6 de maio de 2018 (Art.º 63.º), **e para a Diretiva PNR**, com transposição prevista até 25 de maio 2018 (Art.º 18.º)
  - **designadamente, a desvalorização das garantias relativamente aos "dados de base"**, que teriam uma natureza "meramente técnica", **deixa de fazer** qualquer **sentido** face ao teor da definição de **pessoa** "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial **por referência a um identificador**, como por exemplo um nome, um **número de identificação**, **dados de localização**, **identificadores por via eletrónica** […]" (Art.º 3.º 1 da Diretiva sobre proteção de dados em matéria penal e Art.º 4.º 1 do Regulamento Geral)
- .



Vídeo da apresentação



➔ https://educast.fccn.pt/vod/clips/1boj08c3zn/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5.

Apreensão de correio electrónico e registos de comunicações de natureza semelhante - artigo 17.º da Lei n.º 109/2009, de 15.IX

Rui Cardoso

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5. APREENSÃO DE CORREIO ELECTRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE – ARTIGO 17.º DA LEI N.º 109/2009, DE 15.IX[1]

Rui Cardoso*

I. INTRODUÇÃO

É cada vez mais relevante a utilização como meio de prova no processo penal das mensagens de correio electrónico e de natureza semelhante que são encontradas apreendidas em sistemas informáticos, sistemas esses que são cada vez mais e mais diversos, incluindo agora também objectos que há uns anos eram de pura mecânica, como relógios e automóveis. Não obstante, e apesar de a Lei n.º 109/2009, de 15 de Setembro, autodenominada Lei do Cibercrime (LCC), ter já nove anos, continua escassa a jurisprudência existente sobre algumas das questões, não sendo raro encontrar-se acórdãos de tribunais superiores que ignoram a sua existência.

Propomo-nos abordar integralmente o regime de apreensão de correspondência electrónica, previsto no artigo 17.º da LCC, nomeadamente âmbito objectivo e subjectivo de aplicação, as competências dos órgãos de polícia criminal (OPC's), do Ministério Público e do juiz, prazos, procedimentos práticos e consequências da inobservância das formalidades. Para isso, como veremos, um dos pontos essenciais estará na concretização da correspondente aplicação do regime da apreensão de correspondência previsto no Código de Processo Penal (CPP).

[1] O presente texto constitui mera republicação daquele recentemente publicado na Revista do Ministério Público n.º 153 (Janeiro-Março de 2018), a quem o Centro de Estudos Judiciários agradece a autorização para este efeito concedida.
* Procurador da República e Docente do Centro de Estudos Judiciários.

Apesar de tal puder suceder também na fase de instrução ou mesmo na de julgamento, este meio de obtenção de prova é normalmente utilizado durante o inquérito e é nesses casos que as dúvidas têm surgido, nomeadamente na repartição de competências entre Ministério Público e juiz de instrução. A abordagem às questões procedimentais será assim feita visando apenas a fase de inquérito. Para as posteriores, bastará fazer simples adaptações, retirando o Ministério Público das decisões, havendo uma relação directa entre o juiz e os OPC's.

Frequentemente, o artigo 17.º da LCC tem sido objecto de análise considerando apenas as mensagens de correio electrónico e esquecendo os "registos de comunicações de natureza semelhante", o que não se nos afigura adequado, pois algumas das respostas encontradas poderiam ser válidas para as primeiras, mas não o são para as segundas. Como veremos, não existe fundamento para tal distinção e diferenciação da tutela de direitos.

II. A ORIGEM HISTÓRICA DA LCC

A LCC estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa (STE 185), doravante CCiber, adoptada em Budapeste em 23 de Novembro de 2001, aprovada pela Assembleia da República através da Resolução n.º 88/2009, de 15 de Setembro, e ratificada pelo Decreto de Presidente da República n.º 91/2009, da mesma data – cfr. artigo 1.º.

A Decisão-Quadro n.º 2005/222/JAI do Conselho não contém disposições de natureza processual, contrariamente ao que sucede com a CCiber, que o faz no seu Capítulo II. Sobre a busca e apreensão de dados informáticos armazenados (*search and seizure of stored computer data*, no original inglês) rege o artigo 19.º. Porém, não contém previsão específica similar à do artigo 17.º da LCC, pois não versa directamente a "apreensão de correio electrónico ou registos de comunicações de natureza semelhante".

A inspiração para o artigo 17.º da LCC não está, pois, nem na CCiber, nem na Decisão-Quadro n.º 2005/222/JAI. A origem desse artigo está apenas na Proposta de Lei n.º 289/X/4.ª, tendo ele a mesma exacta redacção que o artigo 19.º desta.

A mera leitura da Exposição de Motivos dessa Proposta de Lei evidencia que o Governo, reconhecendo a "desadequação da ordem jurídica nacional às novas realidades a implementar", não pretendeu fazer uma mera extensão do regime das buscas e apreensões previsto no CPP à prova digital, antes assumindo a vontade de proceder a uma *adaptação desse regime*, superando-o quando necessário: "a forma como a busca e a apreensão estão descritas no CPP exigiam alguma adequação a estas novas realidades". *O legislador propôs-se adaptar estes regimes, não aplicá-los integral e acriticamente*.

III. REGIME GERAL DE APREENSÃO DE DADOS INFORMÁTICOS

Antes de abordarmos o regime *especial* de apreensão de dados informáticos armazenados de mensagens de correio electrónico ou semelhantes, há que conhecer o regime *geral* de apreensão de dados informáticos armazenados, hoje previsto nos artigos 14.º a 16.º da LCC.
Prescreve o n.º 1 do artigo 16.º que "quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.".

O acesso aos dados a apreender pode ser feito através de uma pesquisa, regulada no artigo 15.º, ou através de outro acesso legítimo a um sistema informático. Neste último grupo, devem ser incluídas as perícias, se estas forem realizadas antes da apreensão[2], mas não só. Cremos que aí também se inclui o acesso aos dados que estejam na disponibilidade ou controlo de outra entidade[3], por esta concedido, previsto no n.º 1 do artigo 14.º[4].

Apesar de tal não resultar da letra do n.º 1 do artigo 16.º, os dados informáticos obtidos através da injunção prevista no artigo 14.º também devem ser objecto de apreensão, desde que necessários à produção de prova, tendo em vista a descoberta da verdade. Tal como também as coisas corpóreas voluntariamente entregues devem ser objecto de formal apreensão – artigo 178.º, n.º 1, do CPP.

Como regime-regra, a apreensão deve ser feita por ordem ou autorização da autoridade judiciária competente, que, no inquérito, será o Ministério Público – n.º 1. Os OPC's podem efectuar apreensões, sem prévia autorização da autoridade judiciária, (i) no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º (ou (i.a) voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado, ou (i.b) em casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa), bem como (ii) quando haja urgência ou perigo na demora – n.º 2. Neste caso, as apreensões são sempre sujeitas a validação pela autoridade judiciária (Ministério Público, durante o inquérito), no prazo máximo de 72 horas[5] – n.º 4. O incumprimento desta validação

[2] Assim, DAVID SILVA RAMALHO, *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Almedina, Coimbra, 2017, p. 134-140.
[3] Disponibilidade significa posse física dos dados, com possibilidade de acesso imediato; controlo, ausência de posse física, mas possibilidade de acesso remoto com domínio sobre a sua produção (e não apenas de acesso ou consulta). Cfr. parágrafo 173 do Relatório Explicativo da CCiber: "A expressão "posse ou controlo" refere-se à posse física dos dados em questão no seio do território da Parte que emite a ordem, bem como a situações em que os dados a serem produzidos não se encontram na posse física da pessoa mas sendo possível, contudo, a esta última exercer livremente o seu controlo sobre a produção dos dados a partir do território da Parte emissora da ordem". Reconduzindo as expressões do artigo 14.º, n.º 1, às da CCiber, vd. DAVID SILVA RAMALHO, ob. cit., p. 268-270.
[4] Mas não a intercepções de comunicações electrónicas, prevista no artigo 18.º, que só se aplica aos dados em trânsito.
[5] Este prazo apenas se inicia com a conclusão da pesquisa e elaboração do respectivo auto (se em cumprimento de ordem de autoridade judiciária) ou relatório (na sua ausência), que, dependendo da dimensão e complexidade do sistema informático, poderá demorar mais ou menos tempo, por vezes dias ou semanas. Note-se ainda que a

(ausência ou extemporaneidade) constitui mera irregularidade, pois, contrariamente ao que fez para a pesquisa (artigo 15.º, n.º 4, alínea a)), o legislador não cominou aqui o vício como de nulidade, o que se compreende e é similar ao regime de busca e apreensão do CPP, já que a violação da privacidade dá-se com a pesquisa, não com o acto formal de apreensão.

Estabelece o n.º 3 que "Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.". Aplica-se apenas a dados ou documentos informáticos *já apreendidos*, cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, mas não quaisquer dados pessoais ou íntimos: apenas aqueles que possam pôr em causa a privacidade do respectivo titular ou de terceiro. Durante o inquérito, o Ministério Público deverá apresentar estes dados, apesar de já apreendidos, ao juiz de instrução em suporte autónomo com requerimento fundamentado sobre a sua relevância para a prova dos factos em investigação. O juiz de instrução apreciará o requerido pelo Ministério Público e decidirá sobre a sua junção ou devolução (em caso de apreensão pela forma prevista no n.º 7, alínea a)) ou destruição (em caso de apreensão pela forma prevista no n.º 7, alínea b)).

As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e da actividade médica estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 180.º do CPP; para o exercício da actividade bancária, estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 181.º do CPP; para o exercício da profissão de jornalista, estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista (artigo 11.º da Lei 64/2007) – n.º 5. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do CPP é aplicável com as necessárias adaptações – n.º 6.

Seguindo a previsão do n.º do artigo 19.º da CCiber, o n.º 7 do artigo 16.º prevê, não taxativamente, várias formas de apreensão de dados informáticos, devendo ser escolhida aquela mais adequada e proporcional, tendo em conta os interesses do caso concreto: a) a apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) a realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) a preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; d) ou a eliminação não reversível ou bloqueio do acesso aos dados.

Ao não permitirem o aproveitamento dos dados informáticos como meio de prova no processo, e assim falhando logo o requisito previsto no n.º 1 ("necessários à produção de prova"), as duas últimas não constituem verdadeiras formas de apreensão, antes meios de

pesquisa informática pode iniciar-se no local onde está o sistema (v.g., durante uma busca), aí sendo feito apenas o estritamente necessário para determinar se poderá ou não haver dados relevantes para a prova nesse sistema (havendo, poderá proceder-se à apreensão do sistema informático (computador, *tablet*, etc.), ao abrigo do disposto no artigo 178.º do CPP) e só mais tarde ser concluída, com a procura de *todos* os dados específicos e relevantes aí armazenados e, nesse momento, consequente apreensão ao abrigo do disposto no artigo 16.º da LCC.

protecção de prova ou forma de imposição de limites de acesso a esses dados[6], que por isso devem ser cumulados com uma das duas primeiras formas de apreensão.

Quando a apreensão é feita por cópia dos dados, em suporte autónomo, esta deverá ser feita em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos deverão ser certificados por meio de assinatura digital. Esta assinatura digital não é uma "identificação digital do autor da apreensão"[7], mas antes uma certificação digital de que a cópia é absolutamente igual ao original, não tendo nem mais nem menos *bits*. Isso poderá ser feito por diversas formas técnicas, nomeadamente por *hashing*. Este "é um método de representação de uma colecção de dados através de um número único, que resulta da aplicação de um algoritmo matemático a esses mesmos dados. Dois ficheiros com exactamente a mesma sequência de bits, devem produzir o mesmo código hash quando se utiliza o mesmo algoritmo."[8].

IV. APREENSÃO DE DADOS INFORMÁTICOS ARMAZENADOS DE MENSAGENS DE CORREIO ELECTRÓNICO OU SEMELHANTES

1. Introdução

Dispõe o artigo 17.º da LCC, sob a epígrafe "Apreensão de correio electrónico e registos de comunicações de natureza semelhante" que "quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no CPP.".

O legislador resolveu algumas das questões que se suscitavam na doutrina, nomeadamente quanto às mensagens de correio electrónico armazenadas (*webmail*) ainda nos servidores dos fornecedores de serviço de correio electrónico (ISP), estabelecendo claramente que, sendo possível aceder-lhes legitimamente através de sistema inicial a que se acede (legitimamente), também aí se procede a pesquisa informática (artigos 15.º, n.º 5, e 17.º da LCC), mas a forma de remissão para o regime de apreensão de correspondência previsto no CPP é, em nossa opinião, merecedora de crítica e tem gerado muitas dúvidas na doutrina e na jurisprudência.

[6] Cfr. DAVID SILVA RAMALHO, ob. cit., p. 140-141.
[7] Até porque em 2009, e até este momento, o processo, na fase de inquérito, é apenas o que existe no papel, assim se se excluindo actos processuais electrónicos (artigos 99.º, 100.º e 275.º do CPP), únicos onde uma assinatura digital seria válida.
[8] PEDRO PENHA LEITÃO DA COSTA MARQUES, *Informática Forense - Recolha e preservação da prova digital*, p. 34 e ss., acessível em:
https://repositorio.ucp.pt/bitstream/10400.14/13191/1/Disserta%C3%A7%C3%A3o%20-%20Recolha%20e%20preserva%C3%A7%C3%A3o%20da%20prova%20digital.pdf (consulta em 26.03.2018).

2. O que há a proteger?

A matéria em análise – que respeita às mensagens de correio electrónico, mas também aos registos de comunicações de natureza semelhante – contende com direitos fundamentais, como é frequente em processo penal: directamente, com o direito à inviolabilidade da correspondência e das telecomunicações.

A Constituição da República Portuguesa (CRP), no seu artigo 26.º, n.º 1, a todos reconhece os direitos à identidade pessoal, ao desenvolvimento da personalidade, à reserva da intimidade da vida privada e familiar.

Depois, no seu artigo 34.º, sob a epígrafe "Inviolabilidade do domicílio e da correspondência", consagra que "(…) o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis" (n.º 1) e que "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal." (n.º 4).

Para GOMES CANOTILHO e VITAL MOREIRA[9], "O conteúdo do direito ao sigilo da correspondência e de outros meios de comunicação privada (n.ºs 1 e 4) abrange toda a espécie de correspondência de pessoa a pessoa (cartas postais, impressos), cobrindo mesmo as hipóteses de encomendas que não contêm qualquer comunicação escrita, e todas as telecomunicações (telefone, telegrama, tele-fax, etc.). A garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o «tráfego» como tal (espécie, hora, duração, intensidade de utilização). No âmbito normativo do art. 34° cabe o chamado correio electrónico, porque o segredo da correspondência abrange seguramente as correspondências mantidas por via das telecomunicações. O envio de mensagens electrónicas de pessoa a pessoa («email») preenche os pressupostos da correspondência privada". São manifestações de direitos fundamentais comuns: dignidade da pessoa, desenvolvimento da personalidade, garantia da liberdade individual, autodeterminação existencial e privacidade[10].

O Tribunal Europeu dos Direitos Humanos tem considerado que o direito ao respeito pela correspondência, consagrado no artigo 8.º, n.º 1, da Convenção Europeia dos Direitos Humanos, visa proteger a confidencialidade das comunicações numa ampla gama de situações diferentes, incluindo *mensagens electrónicas* (Copland v. Reino Unido), o uso da *internet* (Copland v. Reino Unido), e *dados armazenados em servidores informáticos* (Wieser e Bicos Beteiligungen GmbH v. Áustria) e *em diferentes suportes* (Petri Sallinen e outros v. Finlândia; Iliya Stefanov v. Bulgária).

A correspondência merece tutela desde o momento do envio, fechada, até ao momento da abertura pelo destinatário. Como afirma COSTA ANDRADE[11], "é precisamente este facto – estar fechada – que define a fronteira da tutela penal do sigilo de correspondência e dos escritos,

[9] *Constituição da República Portuguesa Anotada*, Volume I, Coimbra: Coimbra Editora, 2007, p. 544.
[10] Ob. cit., p. 539.
[11] *Comentário Conimbricense do Código Penal*, Tomo I, Coimbra: Coimbra Editora, 1999, p. 758.

em geral.". Daí que, após aberta, a correspondência fique sujeita ao regime geral de apreensão, previsto no artigo 178.º do CPP.

Por outro lado, e seguindo o mesmo Autor[12], "a tutela do sigilo das telecomunicações, tanto constitucional como processual penal, está (…) *vinculada ao processamento da comunicação sob o domínio da empresa fornecedora do serviço de telecomunicações"*. Esta tutela "só existe enquanto dura o processo dinâmico de transmissão, isto é, até ao momento em que a comunicação entra na esfera de domínio do destinatário. Vale dizer, até ao momento em que ela é recebida e lida pelo destinatário e, neste sentido, termina o processo de telecomunicação à distância. Assim, depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito.". Isto porque essa tutela radica na "*específica situação de perigo* decorrente do domínio que o terceiro detém – e enquanto o detém – sobre a comunicação (conteúdo e dados). Domínio que lhe assegura a possibilidade fáctica de intromissão arbitrária, subtraída ao controlo do(s) comunicador(es).".

No que respeita às mensagens de correio electrónico ou registos de comunicações de natureza semelhantes, como veremos, é muito difícil ou mesmo impossível determinar quando é que terminou a comunicação[13] e se a mensagem já foi ou não aberta/lida[14]. Poderá, assim, não existir segredo de telecomunicações, porque estas podem já ter terminado; não existir segredo de correspondência, porque este pode ter cessado com a abertura.

Não significa isto que não existam direitos fundamentais a tutelar. Recentemente, no acórdão 403/2015[15], o Tribunal Constitucional fez importantíssimas considerações sobre o acesso aos dados das comunicações, *mesmo depois de estas terminadas*, considerando que tal colide com o *direito à autodeterminação comunicativa*, protegido no artigo 34.º da CRP, que "serve para defender vários bens jurídico-constitucionais, entre eles: o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada", e, dentro deste último, para defender "a esfera pessoal perante as ingerências públicas ou privadas, ou seja, o interesse das pessoas que comunicam em impedir ou em controlar a tomada de conhecimento, a divulgação e circulação do conteúdo e circunstâncias da comunicação". O direito ao desenvolvimento da personalidade comporta a liberdade de comunicar e, "nesta dimensão relacional, do "eu" com o "outro", o objeto de proteção é a comunicação individual, isto é, a comunicação que se destina a um recetor individual ou a um círculo de destinatários previamente determinado, liberdade de comunicar que "abrange a faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa".

[12] *"Bruscamente no verão passado", a reforma do Código de Processo Penal – Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora, 2009, p. 158-159.
[13] Existem até programas-cliente de correio electrónico (as versões mais recentes do Outlook) que permitem resgatar e substituir uma mensagem, mesmo que já entregue ao destinatário, desde que este não a tenha aberto.
[14] Motivo por que não há fundamento técnico e, por isso, jurídico, para definir diferentes níveis de tutela com base em considerações de mensagens lidas/não lidas.
[15] Acessível, como todos os demais acórdãos do Tribunal Constitucional citados, em: http://www.tribunalconstitucional.pt/tc/acordaos/.

Pelo exposto, em matéria de apreensão de dados informáticos armazenados de mensagens de correio electrónico ou de registos de comunicações de natureza semelhante, nunca estaremos nem completamente dentro, nem completamente fora quer do âmbito do segredo das telecomunicações, quer do âmbito do segredo da correspondência. Mas estaremos sempre perante perigo de ofensa de direitos fundamentais, como ao desenvolvimento da personalidade, à garantia da liberdade individual, à autodeterminação existencial e privacidade, e por isso com necessidade de tutela adequada.

O legislador deveria então ter criado um regime autónomo e auto-suficiente, com repartição equilibrada de competências entre o Ministério Público e o juiz de instrução, a este reservando o estritamente necessário à garantia de direitos dos visados, adequado às especificidades técnicas das comunicações electrónicas, muito diferentes da correspondência corpórea, e à estrutura acusatória do processo penal.

Porém, com ou sem motivo para tal, o legislador prescreveu ser de aplicar, correspondentemente, o regime de apreensão de correspondência previsto no CPP. É esse regime que há que interpretar correctamente, o que tentaremos fazer adiante.

V. ÂMBITO DE APLICAÇÃO DO ARTIGO 17.º DA LCC

1. Aspectos gerais

O normativo do artigo 17.º aplica-se a mensagens de correio electrónico ou registos de comunicações de natureza semelhante, que, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro. Mais propriamente, *dados informáticos que constituam correio electrónico ou registos de comunicações de natureza semelhante*.

Vimos já que nos "outros acessos legítimos a um sistema informático" devemos incluir, pelo menos, as (i) perícias, se estas forem realizadas antes da apreensão, mas também (ii) o acesso aos dados que estejam na disponibilidade ou controlo de outra entidade, por esta concedido, previsto no n.º 1 do artigo 14.º.

Contrariamente ao que sucede nos casos a que se refere o artigo 16.º, n.º 3, as mensagens de correio electrónico ou semelhantes não estão formalmente apreendidas, pois tal só sucederá se o juiz o determinar. Porém, por regra, tais dados terão já sido objecto de algum dos tipos de apreensão material previstos no artigo 16.º, n.º 7, *supra* analisados, pois só assim haverá "algo" a apresentar ao juiz[16]. Assim apenas não sucederá nos casos em que o juiz estiver presente na pesquisa, perícia ou acesso permitido ao sistema informático, que, na prática, só acontecerá se isso ocorrer no decurso de buscas, domiciliárias ou não domiciliária, por ele presididas.

[16] PEDRO VERDELHO chama-lhe apreensão cautelar ou provisória ("A nova Lei do Cibercrime", Scientia Iuridica, Tomo LVIII, n.º 320, p. 743-744).

Nestas mensagens de correio electrónico ou registos de comunicações de natureza semelhante devem ser incluídas *todas as comunicações, independentemente do seu conteúdo*. Podem, por isso, não ter qualquer conteúdo privado (e.g., *newsletters*, publicidade e correio electrónico não solicitado em geral). Porém, terão de ser necessariamente comunicações entre pessoas humanas, não entre máquinas.

Não devem ser incluídos quaisquer outros dados ("ficheiros") que estejam armazenados no sistema, ainda que eventualmente tenham sido transmitidos por correio electrónico ou de natureza semelhante. Depois de separados da mensagem que os transmitiu, são dados informáticos iguais à generalidade dos demais aí armazenados, podendo nem ser possível determinar a sua origem. Os dados transmitidos e armazenados poderão ser de qualquer natureza – imagem, som (e.g., voz), texto – e podem subsistir armazenados no sistema informático do utilizador depois de ter sido eliminada a mensagem que os transmitiu. Assim deverá suceder, por exemplo, mesmo com facturas electrónicas de serviços de telecomunicações, ainda que detalhadas (com listagens de telefonemas feitos e mensagens de texto enviadas). Aliás, tal como sucede exactamente com aquelas recebidas em papel por correio corpóreo: depois de abertas as cartas, as facturas são documentos iguais a quaisquer outros.

2. O que é o correio electrónico?

O que é o correio electrónico é algo que pode não ser claro[17].

Aí incluímos, sem qualquer dúvida, o correio electrónico transmitido através da *internet*. Por esta via, as mensagens de correio electrónico são transmitidas por meio de servidores de correio electrónico, que são fornecidos por todos os ISP, usando vários protocolos, como SMTP, POP3 ou IMAP. Essas mensagens são transmitidas entre duas pastas dedicadas do(s) servidor(es): do remetente e do destinatário. O remetente envia ou encaminha mensagens de correio electrónico, enquanto o(s) destinatário(s) acede(m) à sua pasta no seu servidor de correio electrónico e aí a lê (e a mantém ou arquiva) ou descarrega para um programa-cliente de correio electrónico no seu sistema informático. Quando transmitidas pela *internet*, as mensagens de correio electrónico integram conteúdo (e.g., texto e ficheiros anexos) e dados de tráfego, contidos nos cabeçalhos técnicos (e.g., percurso percorrido pela mensagem desde a saída da caixa do remetente (*outbox*) até entrar na caixa do destinatário (*inbox*), com registo de cada ponto de passagem e sua data/hora/segundo/fuso horário).

Cremos ser também de incluir na previsão do artigo 17.º o correio electrónico transmitido através de *intranets* (redes de computadores privadas, com vários utilizadores). Tecnicamente, é muito diferente daquele transmitido pela *internet*, mas, para o utilizador, será materialmente idêntico (permite comunicar nos mesmos termos) e por isso deverá ter a mesma protecção.

[17] Sobre a história do correio electrónico, cfr. TOM VAN VLECK, *The History of Electronic Mail* (http://www.multicians.org/thvv/mail-history.html - acesso em 27.03.2018). TOM VAN VLECK é um dos criadores do primeiro programa a isso dedicado.

3. Registos de comunicações de natureza semelhante

Mais complexo é determinar o que são "registos de comunicações de natureza semelhante". Uma interpretação literal poderia levar a que aqui se considerasse incluídos apenas os dados de tráfego de outras transmissões electrónicas de mensagens. De facto, a expressão "mensagens de correio electrónico" inclui, sem dúvida, o conteúdo, enquanto "registos" respeita apenas à ocorrência das comunicações, não ao seu conteúdo. Mais correctamente, o legislador poderia ter dito "mensagens de correio electrónico ou comunicações de natureza semelhante" ou ainda, mais abreviadamente, "mensagens de correio electrónico ou semelhantes". Não o fez, mas não encontramos motivo para excluir o próprio conteúdo dessas mensagens de natureza semelhante: a interpretação contrária levaria ao resultado absurdo, em termos de tutela de direitos, de se conferir maior protecção à apreensão de dados de realização de comunicações (com decisão de juiz de instrução e com exigência de grande interesse para a descoberta da verdade ou para a prova) do que aos de conteúdo (por decisão do Ministério Público, bastando qualquer interesse para a prova).

Estas comunicações de natureza semelhantes podem ser feitas através de um mero serviço telefónico[18], em que o utilizador está identificado através do seu número de telefone[19], ou através da *internet*, utilizando por isso o conjunto de protocolos *TCP/IP*[20], que exigem a atribuição ao utilizador de um *IP Adress*.

No primeiro grupo, incluem-se as *SMS* (*short message service* – serviço de mensagens curtas), as *EMS* (*enhanced messaging service* – serviço de mensagens desenvolvido) e as *MMS* (*multimedia messaging service* – serviço de mensagens multimédia), para cuja intercepção, em tempo real, seria aplicável o disposto nos artigos 187.º e 188.º do CPP.

No segundo, as possibilidades são superiores. Sem preocupações de exaustão (que os nossos imitados conhecimentos técnicos nunca permitiriam e o avanço diário da tecnologia desaconselha até a tentativa de imaginação), afigura-se-nos indubitável que nele devam ser incluídas as comunicações por *IM – Instant messenger* e os *chats ou chatrooms*, para cuja intercepção, em tempo real, seria aplicável o disposto no artigo 18.º da LCC.

Os IM ou programas de mensagens instantâneas *(e.g., Facebook messenger, Skype, Whatsapp, Viber, Snapchat, Telegram*)[21] são programas que, como o próprio nome indica, permitem aos utilizadores o envio e recebimento imediato de mensagens, em tempo real, não exigindo ao destinatário qualquer acto (a não ser ter em funcionamento o seu sistema informático – e.g.,

[18] Serviço ao dispor do público que permite fazer e receber, directa ou indirectamente, chamadas nacionais ou nacionais e internacionais através de um número ou de números incluídos num plano nacional ou internacional de numeração (artigo 3.º da Lei n.º 4/2004 – Lei das Comunicações Electrónicas).
[19] Tecnicamente, *MSISDN - Mobile Station International Subscriber Directory Number* ou Número internacional Identificador de Cliente, público e do conhecimento dos utilizadores. MSISDN = CC + NDC + SN (sendo: CC – Country Code, NDC – National Destination Code, SN – Subscriber Number). Consultar: https://www.anacom.pt/render.jsp?categoryId=337614 (acesso em 27.03.2018).
[20] Protocolos de comunicação entre computadores em rede, significando TCP - *Transmission Control Protocol* e IP - *Internet Protocol*.
[21] Que, nesta data, serão usadas por mais de metade dos portugueses que têm telemóvel – https://tek.sapo.pt/noticias/telecomunicacoes/artigos/apps-de-instant-messaging-usadas-por-mais-de-metade-dos-portugueses-que-tem-telemovel (acesso em 27.03.2018).

computador, *tablet* ou *smartphone*). Para além do texto, podem permitir a transmissão de ficheiros, a conversação por voz ou a videoconferência. Porém, por regra, as mensagens transmitidas ficam armazenadas nos sistemas dos intervenientes, podendo, por isso, tais dados ser apreendidos.

Os chats ou *chatrooms* (em português, salas de conversação), são locais *online*[22] onde duas ou mais pessoas se podem encontrar virtualmente e trocarem mensagens e ficheiros, que podem ser utilizados para finalidades lícitas, mas também ilícitas, sendo frequentemente usados em redes de partilha de pornografia infantil. Podem ser abertos/públicos ou fechados/privados. Os registos dessas comunicações podem ser guardados por qualquer utilizador (se não for possível outra forma, pelo menos o conseguirão através de fotografias dos écrans – *printscreen*) dando ao ficheiro uma qualquer terminação para o ocultar (e.g., de folha de cálculo ou de apresentação multimédia).

4. Mensagens de correio electrónico ou semelhantes abertas e não abertas

O artigo 17.º da LCC não faz qualquer distinção entre mensagens de correio electrónico ou semelhantes abertas e não abertas[23].

Como consta do seu Preâmbulo, a CCiber leva em consideração a Recomendação do Comité de Ministros do Conselho da Europa R (95) 13, relativa a problemas de processo penal relacionados com tecnologia de informação. Esta, no seu ponto I.2., recomenda aos governos dos Estados-membros que

> *"criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein*."

Ou seja, também esta recomendação não faz qualquer distinção entre tipos de dados informáticos, e.g. dos de correio electrónico face aos demais.

A CCiber não ignora os problemas que podem ser suscitados com as mensagens não abertas, mas não nos termos que em Portugal têm sido colocados. Nesse sentido, veja-se o parágrafo 190 do seu Relatório Explicativo, onde se lê:

> "O Artigo 19º é consagrado aos dados informatizados armazenados. A este respeito, é colocada a questão que incide sobre o facto de se uma *mensagem de correio electrónico não aberta, em espera na caixa de correio de um fornecedor de serviços de*

[22] Noutros tempos, os *chats* eram feitos através de programas existentes para essa finalidade (como o *IRC – Internet Relay Chat*), hoje completamente em desuso por força dos *IM*.
[23] Assim, também DAVID SILVA RAMALHO, ob. cit., p. 278-279, e o Ac. do TRG de 29.03.2011, P. 735/10.0GAPTL- A.G1 (MARIA JOSÉ NOGUEIRA).

> *Internet, até que o respectivo destinatário efectue o descarregamento para o seu sistema informático*, deverá ser considerada como constituindo dados armazenados ou dados em curso de transferência. Ao abrigo da legislação adoptada por algumas Partes, a referida mensagem de correio electrónico faz parte integrante de uma comunicação, pelo que o seu conteúdo apenas poderá ser conhecido mediante a aplicação do poder de intercepção, enquanto que, segundo outros sistemas jurídicos, a dita mensagem se considera pertencer ao domínio dos dados armazenados aos quais se refere o Artigo 19º. Assim, as Partes deverão proceder a uma revisão das suas leis relativas a esta matéria, por forma a determinar qual é a visão mais adequada no âmbito dos seus sistemas jurídicos internos." (realce nosso).

Ou seja, para a CCiber, a questão apenas se pode colocar relativamente a mensagens que estão nos servidores dos ISP, não as já descarregadas para os sistemas informáticos dos seus destinatários. Isto porque a CCiber apenas distingue entre dados informáticos em trânsito (a recolher em tempo real – artigos 20.º e 21.º) e dados informáticos armazenados (artigo 19.º).

O legislador nacional tomou posição sobre esta questão, considerando tais dados incluídos na previsão do artigo 17.º da LCC (dados armazenados) e não na do artigo 18.º (intercepção em tempo real). É indiscutível a correcção da opção da nossa lei: no nosso sistema (artigos 187.º e 188.º do CPP e artigo 18.º da LCC) só os dados em trânsito podem ser interceptados – por estas vias, nunca se poderia apreender os dados armazenados nos servidores de correio electrónico dos ISP[24].

Recorde-se que o artigo 15.º, n.º 5, da LCC permite que, quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.ºs 1 e 2, e que o próprio artigo 17.º prevê expressamente que as mensagens de correio electrónico ou semelhantes possam estar noutro sistema informático a que seja permitido o acesso legítimo a partir do primeiro, o que se aplica precisamente, mas não só, aos servidores de correio electrónico[25], independentemente do local onde estejam alocados os respectivos dados[26]. Apenas dessa forma se poderá aceder a essas mensagens e a violação da privacidade do visado é a mesma que sucederia se essas estivessem já descarregadas para o seu computador através de um programa-cliente de correio electrónico.

[24] Pode não ser líquido determinar se uma mensagem está ou não descarregada dos servidores de ISP para o sistema do utilizador. Desde logo, porque, após o *download*, as mensagens ficarão ou não no servidor do ISP conforme for a vontade do utilizador. Podendo assim as mensagens ter sido descarregadas num dos suportes do utilizador que não o pesquisado e, assim, não ser conhecido que já houve esse *download*. Por outro lado, as mensagens poderão ser descarregadas apenas parcialmente: apenas o cabeçalho e o corpo, deixando os anexos no servidor, que só serão descarregados se e quando o utilizador o desejar. Daí que não deva fundar-se nesse aspecto qualquer solução jurídica para tutela de direitos.

[25] Assim, PEDRO VERDELHO, ob. cit., p. 742.

[26] Quanto à irrelevância, neste aspecto, da territorialidade, cfr. DAVID SILVA RAMALHO, "A recolha de prova em sistemas de computação em nuvem", in Revista do Direito Intelectual, N.º 2, 2014, p. 142-146. No mesmo sentido, também PEDRO DIAS VENÂNCIO, *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora, 2011, p. 120.

Não é juridicamente correcto, nem tecnicamente adequado, interpretar o artigo 17.º da forma diferente para mensagens abertas e mensagens não abertas.

O *aberto* ou *não aberto* ou, mais correctamente, *lido* ou não *lido*, não é uma qualquer forma de protecção do conteúdo da mensagem, contrariamente ao que sucede com os envelopes no correio corpóreo[27]. Não são envelopes ou invólucros das mensagens, mas simples filtros que o utilizador pode definir (de acordo com as suas preferências ou critérios) para mais facilmente gerir o volume de mensagens de correio electrónico recebidas. A mensagem de correio electrónico, "por natureza, não é *fechada*, não é *envelopável*, não é unívoca quanto ao número de destinatários e não circula em ambiente seguro (…). E, sobretudo, é, no seu estado natural imaterial."[28].

Alguns dos prestadores de serviço de correio electrónico continuam a ter regimes de *lido/não lido*, mas que, contrariamente ao que sucede com a correspondência corpórea, podem ser facilmente alteráveis (e infinitamente) pelo utilizador, com um clique. O correio electrónico pode ser arquivado pelo destinatário sem ser lido; pode ser arquivado juntamente com mensagens enviadas e até rascunhos de mensagens eventualmente a enviar. Como distinguí-los?

Por outro lado, esses filtros de "lido/não lido" não existem sequer em vários telefones móveis/sistemas operativos de *smartphones* para as *SMS/EMS/MMS*, em vários dos programas de *instant messaging* e nos *chats*.

Ainda, hoje, os utilizadores podem receber – e, em regra, recebem – o correio electrónico simultaneamente numa multiplicidade de plataformas: computadores (fixos e portáteis), *tablets*, *smartphones*, automóveis, relógios, etc.. Numas, as mensagens poderão constar como lidas, noutras, como como não lidas, dependendo das definições de sincronização possíveis e adoptadas.

Não há, então, reais bases para fundamentar nessa ilusão do lido/não lido diferentes níveis de tutela jurídica das mensagens de correio electrónico ou semelhantes. Divergimos assim de JOÃO CONDE CORREIA[29] e ainda de PAULO DÁ MESQUITA[30] quando defende precisamente que, ao

[27] Assim, VÂNIA COSTA RAMOS, "Âmbito e extensão do segredo das telecomunicações (acórdão do segundo senado do Tribunal Constitucional Federal Alemão, de 2 de março de 2006)", RMP n.º 112, p. 154-155.
[28] ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", Polícia e Justiça, III Série, n.º 7, Janeiro-Junho de 2006, p. 214.
[29] "Prova digital: as leis que temos e a lei que devíamos ter", RMP n.º 139, p. 40, onde escreve que "uma leitura integrada e coerente, que acentue as inevitáveis semelhanças com os escritos tradicionais e as suas necessidades de tutela, tenderá todavia, apesar daquele elemento gramatical [do artigo 17.º], a excluir este correio, considerando-o como um mero documento e facilitando a sua apreensão: será para o efeito suficiente a intervenção legitimadora do magistrado do Ministério Público (art. 16.º da Lei n.º 109/2009). (…) A proteção do sigilo das comunicações (sejam elas por correio tradicional ou através dos meios que o progresso disponibilizou) deve terminar quando a mensagem chega ao seu destinatário e aquele processo de transmissão se encontra concluído. A partir desse momento (conclusão efetiva do processo de transmissão) o destinatário dispõe dos meios necessários a evitar a intromissão estadual. Ele já não está vulnerável, sujeito às falhas de reserva do operador ou à curiosidade estadual.".
[30] "Prolegómeno sobre prova electrónica e intercepção de comunicações no direito processual penal português – o Código e a Lei do Cibercrime", in: Processo Penal, Prova e Sistema Judiciário, Coimbra: Coimbra Editora, 2010, p. 118.

determinar a aplicação do regime de apreensão de correspondência do CPP, se exclui da tutela especial as mensagens de correio electrónico já acedidas pelo destinatário.

VI. A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Antes de determinarmos qual a dimensão da remissão para o regime de apreensão de correspondência previsto no CPP, há que dizer algumas palavras sobre este.

1. A apreensão de correspondência no CPP

Prescreve o artigo 179.º do CPP, sob a epígrafe "Apreensão de correspondência":

> **1** – Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que:
>
> > **a)** A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa;
> > **b**) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e
> > **c)** A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.
>
> **2** – É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime.
>
> **3** – O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

Relevante é ainda o artigo 252.º, incluído no capítulo das medidas cautelares e de polícia, que dispõe:

> **1** – Nos casos em que deva proceder-se à apreensão de correspondência, os órgãos de polícia criminal transmitem-na intacta ao juiz que tiver autorizado ou ordenado a diligência.

2 – Tratando-se de encomendas ou valores fechados susceptíveis de serem apreendidos, sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora, os órgãos de polícia criminal informam do facto, pelo meio mais rápido, o juiz, o qual pode autorizar a sua abertura imediata.

3 – Verificadas as razões referidas no número anterior, os órgãos de polícia criminal podem ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações. Se, no prazo de quarenta e oito horas, a ordem não for convalidada por despacho fundamentado do juiz, a correspondência é remetida ao destinatário.

Este regime tem várias dimensões normativas (para o que ora releva):

1. Competência – apenas o juiz é competente para autorizar ou ordenar, por despacho, a apreensão;

2. Âmbito objectivo – apreensão de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, mesmo nas estações de correios e de telecomunicações;

3. Redução do âmbito objectivo – a apreensão de correspondência só é meio de obtenção de prova admissível para crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos;

4. Âmbito subjectivo – a correspondência tem de ser expedida pelo suspeito/arguido ou lhe ser dirigida, mesmo que sob nome diverso ou através de pessoa diversa;

5. Redução do âmbito subjectivo – a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor só é admissível se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime;

6. Necessidade probatória – tem de haver razões para crer que a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova;

7. Procedimentos após a apreensão – os OPC's transmitem a correspondência intacta ao juiz que tiver autorizado ou ordenado a diligência e este é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova;

8. Invalidade – proibição de prova ou irregularidade[31].

2. Conjugação do artigo 17.º da LCC com o artigo 179.º do CPP

O artigo 17.º determina a *correspondente* aplicação do regime de apreensão de correspondência do CPP, *não a aplicação integral*. Esta só deve ser feita naquilo que não contrariar o já previsto na própria LCC; a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC. Como vimos já, foi intenção do legislador adaptar às novas realidades a busca e a apreensão previstas no CPP, não aplicá-los integral e acriticamente.

Deste modo, e esquematicamente:

- No CPP, o âmbito objectivo é o de correspondência em trânsito ou ainda não aberta; na LCC, todas as mensagens de correio electrónico ou semelhantes, nos termos supra expostos, não havendo verdadeiramente regime aberto-lido e fechado-não lido;

- No CPP, a apreensão de correspondência só é meio de obtenção de prova admissível para crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos; na LCC, não há catálogo – por força do expressamente previsto no artigo 11.º, aplica-se a processos relativos a crimes (a) previstos nessa lei, (b) cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, ou seja, em abstracto, a todos os tipos de crime;

- No CPP, a correspondência tem de ser expedida pelo suspeito/arguido ou lhe ser dirigida, mesmo que sob nome diverso ou através de pessoa diversa; na LCC, pode

[31] Acompanhamos PAULO PINTO DE ALBUQUERQUE (*Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* Lisboa: Universidade Católica Editora, 3.ª Edição, p. 494) quando considera que existem proibições de prova, por violação do disposto no n.º 3 do artigo 126.º, quando há apreensão sem autorização judicial, quanto à apreensão de correspondência entre o arguido e o seu defensor, excepto se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime, e ainda quanto à valoração de correspondência restituída. Porém, não o fazemos quanto à existência de nulidade prevista no artigo 120.º, n.º 2, alínea d) (dependente de arguição) quando existe omissão do exame. Este vício apenas ocorre *quando o inquérito ou instrução são insuficientes* por não terem sido praticados actos legalmente obrigatórios, não apenas por não terem sido praticados actos legalmente obrigatórios. Estes actos deverão ser apenas os que respeitem à finalidade de inquérito (diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas – artigo 262.º, n.º 1) ou da instrução (comprovação judicial da decisão de deduzir acusação ou de arquivar o inquérito em ordem a submeter ou não a causa a julgamento – artigo 286.º, n.º 1). Se assim não fosse, todas as inobservâncias das prescrições legais no inquérito e na instrução integrariam esta nulidade – e o princípio da tipicidade do artigo 118.º seria subvertido e deixaria de fazer sentido. A omissão do exame pelo juiz, bem como se este ordenar a apreensão, mas depois ordenar ao OPC que primeiro tome conhecimento do conteúdo da correspondência e só depois fundamentar a sua relevância e junção ao processo, constituem apenas irregularidades.
Note-se ainda que não há qualquer cominação de nulidade na letra da primeira parte do n.º 3 do artigo 179.º e que a prova é obtida com a apreensão ordenada pelo juiz – e é com esta que se verifica a *intromissão na correspondência* –, não com o conhecimento do seu teor por parte do Ministério Público ou dos OPC's, sendo por isso de afastar a proibição de prova prevista no artigo 126.º, n.º 3.

respeitar a qualquer pessoa (mais uma vez, o artigo 11.º não faz qualquer restrição de âmbito subjectivo) [32/33];

- No CPP e na LCC, o critério da necessidade para a prova é o mesmo: grande interesse para a descoberta da verdade ou para a prova;

- O artigo 17.º da LCC não tem previsão sobre invalidade, pelo que deve operar a remissão para o CPP, aplicando-se o regime do artigo 179.º supra referido;

- O artigo 17.º da LCC não tem previsão sobre a apreensão de correspondência electrónica ou semelhante entre o arguido e o seu defensor, pelo que deve operar a remissão para o CPP (só será admissível se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime);

- No que respeita aos procedimentos, no CPP os OPC's transmitem a correspondência intacta ao juiz que tiver autorizado ou ordenado a diligência e é este que procede à aberta e primeiro toma conhecimento do seu conteúdo; na LCC, durante o inquérito, o Ministério Público, depois de tomar conhecimento do seu conteúdo, deve apresentar ao juiz suporte com as mensagens de correio electrónico ou semelhantes cautelarmente apreendidas (ou melhor, os dados informáticos que as constituem), juntamente com requerimento fundamentado para apreensão daquelas que considere de grande interesse para a descoberta da verdade ou para a prova, após o que o juiz apreciará, tomando conhecimento do seu conteúdo, e decidirá autorizar ou não autorizar a apreensão formal.

[32] Assim, PAULO DÁ MESQUITA, *Prolegómeno…*, p. 108 e ss.. Contra, RITA CASTANHEIRA NEVES, *As ingerências nas comunicações electrónicas no processo penal*, Coimbra Editora, 2011, p. 274-275.

[33] A aplicação do âmbito subjectivo do regime de apreensão de correspondência afronta directamente o artigo 14.º da CCiber, que o n.º 1 do artigo 11.º da LCC fielmente reproduz. Como explicitado do parágrafo 141 do Relatório Explicativo, "cada Parte deverá aplicar os poderes e procedimentos descritos em conformidade com a presente Secção a: (i) infracções penais definidas de acordo com a Secção 1 da Convenção; (ii) outras infracções penais cometidas por meio de um sistema informático; e (iii) à recolha de provas sob a forma electrónica relativamente a uma infracção penal. Assim, para efeitos de investigações criminais ou acções penais específicas, os poderes e procedimentos referidos nesta Secção deverão ser aplicados às infracções definidas de acordo com a Convenção, a outras infracções penais cometidas por meio de um sistema informático, e à recolha de provas sob a forma electrónica relativamente a uma infracção penal.". A este âmbito a CCiber faz apenas duas restrições: quanto à intercepção de dados de conteúdo (artigo 21.º), que deverá ser limitado a um conjunto de infracções graves a ser determinado pela legislação nacional, e quanto à recolha de dados de tráfego em tempo real (artigo 20.º), que cada Estado-Parte poderá reservar-se o direito de aplicar somente às infracções ou categorias de infracções especificadas na reserva formulada, desde que o conjunto das referidas infracções ou categorias de infracções não seja mais restrito do que o conjunto das infracções às quais se aplicam as medidas de intercepção mencionadas no artigo 21.º. Sublinhe-se que nenhuma destas duas excepções respeita a dados já armazenados: são sempre dados em circulação, em tempo real. As normas da CCiber têm valor supra-legal e obrigam a que a interpretação e aplicação da lei nacional sejam feitas em seu respeito – artigo 8.º, n.º 2, da CRP.

3. Procedimentos de selecção e apreensão

3.1. Posições discordantes

Este último aspecto, procedimental, é, na fase de inquérito, o mais polémico e é aquele que motiva o maior dissenso nas escassas doutrina e jurisprudência existentes sobre estas matérias.

Na jurisprudência, estão publicados três acórdãos sobre a matéria.

O recente acórdão do TRL de 06.02.2018, P. 1950/17.0 T9LSB-A.L1-5 (JOÃO CARROLA)[34] considerou que a LCC remete expressamente para o regime geral previsto no CPP, sem redução do seu âmbito, antes se impondo a sua aplicação na sua totalidade, pelo que, sob pena de nulidade, se exige que seja o juiz de instrução o primeiro a tomar conhecimento do conteúdo das comunicações. No mesmo sentido, foi o acórdão do TRL de 11-01-2011, P. 5412/08.9TDLSB-A.L1 (RICARDO CARDOSO). Em ambos os casos, foi dado provimento a recursos do Ministério Público.

Em sentido contrário, existe o acórdão do TRG de 29.03.2011, P. 735/10.0GAPTL- A.G1 (MARIA JOSÉ NOGUEIRA), em que se considerou ser de aplicar à apreensão de uma *SMS* o disposto no artigo 17.º da LCC, mas podendo o Ministério Público aceder ao seu conteúdo antes da decisão de apreensão [formal] do juiz de instrução.

Na doutrina, RITA CASTANHEIRA NEVES[35] defende que a remissão para o regime de apreensão da correspondência do CPP respeita também ao facto de ter de ser o juiz que tiver autorizado ou ordenado a diligência a primeira pessoa a tomar conhecimento do conteúdo do correio electrónico e demais registos de comunicações apreendidos, mandando-os juntar ao processo se os considerar relevantes. SANTOS CABRAL[36] igualmente considera ser de aplicar integralmente o regime de apreensão de correspondência do CPP.

PAULO DÁ MESQUITA[37] manifesta concordância com a remissão para o regime da apreensão de correspondência do CPP (embora, como vimos, restringindo muito o campo de aplicação do artigo 17.º da LCC, considerando que respeita apenas a mensagens não lidas), afirmando que parece estar pressuposto a apresentação das comunicações ao juiz sem prévio acesso policial. Porém, não aprofunda a problemática do âmbito dessa remissão.

É PEDRO VERDELHO[38] quem maior tratamento dá à questão. Defende esse Autor que o regime da apreensão de correspondência do CPP deve ser feito com as necessárias adaptações: a primeira, respeitando à possibilidade de apreensão cautelar das mensagens de correio electrónico ou semelhantes sem autorização prévia do juiz de instrução (sendo a existência de forma legal de acesso ao meio informático onde estavam armazenadas a única

[34] Acessível, como todos os demais acórdãos dos tribunais comuns citados, em www.dgsi.pt.
[35] Ob. cit., p. 274-275.
[36] *Código de Processo Penal Comentado*, AAVV, Coimbra: Coimbra Editora, 2016, 2.ª edição, p. 708.
[37] *Prolegómeno…*, p. 117 e ss., nota 71.
[38] Ob. cit., 744-745.

exigência legal para essa apreensão cautelar); depois, que não se exige que seja o juiz o primeiro a ter conhecimento de todas as mensagens (a letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não).

3.2. Nossa posição

Com a vénia devida, acompanhamos PEDRO VERDELHO, aprofundando a sua argumentação e acrescentando outra.

Fundamos a nossa posição em argumentos de (i) literalidade, de (ii) coerência do sistema de tutela de direitos, de (iii) diferenças de natureza entre o correio corpóreo e correio electrónico ou semelhante, e, finalmente, na (iv) imposição constitucional de respeito pela estrutura acusatória do nosso processo penal.

i. Letra da lei

Em primeiro lugar, a letra do artigo 17.º oferece bons argumentos para a posição que defendemos.

Se fosse intenção do legislador aplicar integralmente o regime de apreensão da correspondência do CPP, bastar-lhe-ia ter dito que "à apreensão de mensagens de correio electrónico ou registos de comunicações de natureza semelhante é aplicável o regime de apreensão de correspondência previsto no CPP". Não o fez. Porquê seleccionar e repetir no artigo 17.º da LCC apenas um dos requisitos já previstos no artigo 179.º do CPP (grande interesse para a descoberta da verdade ou para a prova)? Nessa interpretação, seria redundante.

Outro argumento na letra do artigo 17.º está no segmento "o juiz pode autorizar ou ordenar, por despacho", expressão que o CPP utiliza frequentemente a propósito da competência do juiz de instrução face a vários meios de prova ou de obtenção de prova, desde logo no artigo 269.º[39]. Na instrução, competirá ao juiz de instrução ordenar a apreensão; no inquérito, apenas autorizá-la[40/41].

No inquérito, o juiz de instrução autoriza a apreensão, mas é o Ministério Público que a ela procederá (ou, por regra, determinará OPC a fazê-lo). Note-se que a apreensão poderá não ser de tudo o requerido pelo Ministério Público e assim haverá necessidade de proceder à apreensão apenas daquilo que for autorizado através da forma prevista no artigo 16.º, n.º 7, alínea b) (realização de uma cópia só com esses dados), para que será necessário

[39] O n.º 1 deste artigo, que se aplica apenas ao inquérito, usa ambos os verbos, respeitando o ordenar às alíneas a) e b) (efectivação de perícias, nos termos do n.º 3 do artigo 154.º, e efectivação de exames, nos termos do n.º 2 do artigo 172.º), pois aí a acção deve impor-se perante terceiros – aqueles que assim ficarão obrigados a submeter-se a esses meios de prova –, não podendo, assim, ser apenas "autorizar". Não infirma, pois, a nossa argumentação.
[40] Quando o meio de obtenção de prova apenas é admissível no inquérito – e.g., as intercepções telefónicas (artigo 187.º do CPP) e as intercepções de comunicações electrónicas (artigo 18.º da LCC), o legislador refere sempre apenas a competência do juiz de instrução para autorizar, nunca para ordenar.
[41] Assinale-se a diferença de redacção face ao n.º 3 do artigo 179.º, onde é dito que "o juiz faz juntar ao processo".

conhecimentos técnicos e ferramentas informáticas que os magistrados dificilmente possuirão. Autorizar, como verbo transitivo, significa conceder licença para algo, conferir autoridade a, permitir, validar, apoiar[42]. No caso, pressupõe, pois, que a iniciativa é de outrem, do Ministério Público, e que é desse a selecção das comunicações cuja apreensão se autorizará ou não. A não ser assim, o juiz de instrução nunca se limitaria a autorizar, antes sempre ordenaria a apreensão, deixando sem sentido aquilo que o legislador expressamente inseriu na redacção do artigo 17.º.

Ora, o Ministério Público não pode requerer a apreensão das mensagens de correio electrónico ou semelhantes que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova se não as conhece. Não as conhecendo, não haveria verdadeiro requerimento, mas apenas um impulso para uma decisão do juiz de instrução a que o Ministério Público seria completamente alheio. Levaria até a uma subversão de papéis: depois do juiz de instrução "autorizar" a apreensão, o Ministério Público sempre poderia não usar essa autorização, não procedendo à apreensão, v.g., por a considerar irrelevante para a descoberta da verdade ou a prova. A não ser assim, estaria o juiz de instrução a impor ao Ministério Público a utilização de concretos meios de prova.

Evidentemente, e como aprofundaremos *infra*, isso não respeita minimamente a estrutura acusatório do processo penal consagrada na Constituição.

Sublinhe-se ainda que, apesar de o artigo 179.º do CPP e o artigo 17.º da LCC utilizarem diferentes nomenclaturas para os dois momentos do procedimento – (1.º) empossamento da comunicação e (2.º) sua admissão como meio de prova no processo –, estes não são substancialmente diferentes nos dois diplomas: assim, no CPP chama-se apreensão ao empossamento e junção ao processo à admissão como meio de prova; na LCC, não se nomeia o empossamento, mas há uma verdadeira apreensão nos termos do artigo 16.º, n.º 7, ainda que cautelar ou provisória, e a admissão como meio de prova é denominada de apreensão. Porém, e esse é aspecto de grande relevância, o CPP reserva ao juiz a competência para ordenar o empossamento, enquanto na LCC essa competência é, no inquérito, do Ministério Público, podendo os OPC's fazê-lo apenas nas situações previstas no artigo 16.º, n.º 2.

ii. Coerência do sistema de tutela de direitos

Se devemos presumir que o legislador soube exprimir o seu pensamento em termos adequados, também temos de presumir que consagrou as soluções mais acertadas – artigo 9.º, n.º 3, do Código Civil. Estas não seriam as mais acertadas se fossem radicalmente incoerentes entre três artigos (seguidos!) no mesmo diploma, oferecendo uma menor tutela a situações potencialmente mais lesivas dos direitos fundamentais.

Porém, é a isso mesmo que conduz a interpretação que defende que, no inquérito, o juiz de instrução é sempre o primeiro a tomar conhecimento das mensagens de correio electrónico ou

[42] "Autorizar" in Dicionário infopédia da Língua Portuguesa [em linha]. Porto: Porto Editora, 2003-2018. [consulta em 03.04.2018]. Disponível na Internet: https://www.infopedia.pt/dicionarios/lingua-portuguesa/autorizar.

semelhantes. Nos casos mais graves para a privacidade dos artigos 16.º, n.º 3[43], e 18.º, os OPC's e o Ministério Público podem e devem tomar primeiro conhecimento do conteúdo; nos casos menos graves, quando pode nem sequer existir qualquer violação de privacidade (aplica-se a todas as mensagens de correio electrónico ou semelhantes, independentemente do seu conteúdo), é o juiz de instrução que o deve fazer. Não encontramos razão de política criminal que sustente tal diferença.

Não se diga que, no inquérito, também nos casos do artigo 16.º, n.º 3, deve ser o juiz de instrução o primeiro a tomar conhecimento desses dados: só com o conhecimento dos mesmos é possível determinar se são ou não susceptíveis de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro e, depois, suscitar a intervenção do juiz de instrução – se assim não fosse, teria de ser sempre o juiz de instrução o primeiro a tomar conhecimento de todos os dados informáticos. Não é isso que ficou expressamente consagrado nos artigos 15.º e 16.º da LCC.

Por outro lado, quando há intercepção das comunicações electrónicas, também os OPC's e o Ministério Público deles tomam conhecimento antes do juiz de instrução, podendo fazê-lo até em tempo real (no decurso das comunicações) – artigo 188.º, n.ºs 1 a 4, do CPP, *ex vi* do artigo 18.º, n.º 4, da LCC. Os dados podem ser os mesmos: os das comunicações electrónicas e semelhantes, que, mais tarde, já armazenados, podem ser apreendidos nos termos do artigo 17.º. Para além dos aspectos tutelados pelo artigo 17.º, está aqui em causa o próprio sigilo das telecomunicações. Não se compreende que, durante a comunicação electrónica, os OPC's e o Ministério Público possam dela tomar conhecimento primeiro, mas não o possam fazer já depois de esta terminada.

Não colhe o argumento de que na intercepção houve já prévia intervenção do juiz de instrução, pois sem a sua autorização aquela não é possível. É que o problema não está no acesso, mas no conhecimento dos dados por parte dos "*não juiz de instrução*": e esse é o mesmo, quer os dados estejam em transmissão, quer estejam já armazenados. A ofensa à privacidade do titular é a mesma.

Note-se que, mesmo com a interpretação por nós defendida, o regime continuará com uma significativa incoerência: para as intercepções telefónicas e as intercepções de comunicações electrónicas a selecção das conversações ou comunicações que valerão como prova é, em primeira linha, competência do Ministério Público (artigo 188.º, n.º 9, do CPP), enquanto que para os dados dessas mesmas comunicações já armazenados a competência será sempre do juiz. Mas essa foi indiscutivelmente a intenção do legislador. Não sendo inconstitucional, não pode ser afastada a aplicação da norma.

iii. Correio electrónico e correio corpóreo

Como vimos, a apreensão de correspondência e a apreensão de mensagens de correio electrónico ou semelhantes não afectam exactamente os mesmos direitos fundamentais e

[43] Que, por exemplo, podem abranger fotografias íntimas, registos clínicos, registos bancários, etc.

existem diferenças substanciais entre o correio corpóreo e as mensagens de correio electrónico ou semelhantes e, consequentemente, com o campo de aplicação do artigo 179.º do CPP e do artigo 17.º da LCC.

A remissão acrítica para o regime da apreensão de correspondência do CPP não oferece qualquer tutela para as situações em que a mensagem de correio electrónico está simultaneamente em vários sistemas do remetente e do(s) destinatários(s), pois tal não pode suceder com a correspondência corpórea (ou está em trânsito ou está já entregue ao único destinatário e num único local), contrariamente ao que sucede com o correio electrónico, em que o remetente fica, por regra, com a mensagem que enviou. Antes de ser expedida a carta ou encomenda, não há correspondência: há um objecto (e.g., folhas de papel) dentro de um invólucro (e.g., um envelope). Às mensagens de correio electrónico enviadas e aos rascunhos não poderia nunca aplicar-se o regime de apreensão de correspondência – a remissão para o regime do CPP é, por isso, inadequada. Porém, essas mensagens/rascunhos são dados informáticos armazenados num sistema informático, não sendo excluídos da previsão do artigo 17.º. Nessa situação, o fundamento para o juiz de instrução ser o primeiro a delas tomar conhecimento tem ainda menos sustentação, sob pena de ainda irmos além da previsão do artigo 179.º, sem qualquer base legal.

A diferença de natureza entre os dois referidos tipos de "correspondência" manifesta-se ainda noutros aspectos. A identificação de um objecto como "cartas, encomendas, valores, telegramas ou qualquer outra correspondência", a que se aplica o disposto no artigo 179.º do CPP, é feita sem qualquer necessidade de tomar conhecimento do seu conteúdo; porém, em muitos casos, é impossível saber o que é ou não "mensagem de correio electrónico" ou "registo de comunicações de natureza semelhante" sem tomar conhecimento do seu conteúdo.

Desde logo, as mensagens de correio electrónico ou semelhantes podem ser guardadas, individualmente ou em grupo, podendo o utilizador fazê-lo em diferentes tipos de ficheiro e com os nomes que entender[44]. Nesses casos, só com a abertura de cada um desses ficheiros será possível saber se contêm ou não mensagens de correio electrónico ou semelhantes. Não se nos afigura admissível considerar que o artigo 17.º só se aplica às mensagens que se encontram no respectivo programa utilizado para as transmitir: isso seria reduzir o âmbito da sua tutela sem qualquer apoio na letra da lei e sem qualquer fundamento material para tal. Seria o mesmo que considerar que, para o correio corpóreo, apenas se aplica o regime do artigo 179.º à correspondência em trânsito ou ainda na caixa de correio do destinatário, não a partir do momento em que deste local fosse retirada.

Depois, como vimos, a própria letra da lei prevê a possibilidade de o "encontrar" os dados ocorrer durante uma perícia: esta, por definição, consiste na percepção e análise dos dados – ou seja, obriga a tomar conhecimento do seu conteúdo. Não raras vezes, a perícia deve ser

[44] Poderá gravá-los como páginas web (e.g., html), ficheiros de texto (e.g., docx, doc, txt, tiff, rtf), de arquivo de imagem (pdf), como imagem (e.g., jpeg), etc. Os ficheiros de arquivo de correio electrónico do programa *Outlook* têm a terminação .pst, mas, depois de gravado, o utilizador pode alterar tal terminação, não permitindo a outros conhecer que esse ficheiro respeita a arquivo de correio electrónico.

feita no momento da pesquisa, com o sistema ligado, durante a busca a um local, sob pena de se perderem os dados relevantes. Pense-se, por exemplo, num situação em que a pesquisa revela (ou o seu possuidor declara nesse momento) que o sistema que enviou determinada mensagem electrónica foi *hackeado* (e que assim estava controlado externamente), ou que as imagens que estavam nesse sistema não foram por ele recebidas, mas sim aí colocadas por outros[45]: nesses casos, será necessário proceder a uma perícia imediata (*live forensics*) para determinar o que está a acontecer naquele momento naquele sistema, com o mesmo em execução e com captura de todos os dados voláteis, como a configuração actual da máquina e os dados na memória RAM, dados que seriam perdidos assim que a máquina fosse desligada. Essa *análise forense ao vivo* capturará todos os processos em execução e, portanto, poderá apurar se um *vírus* estiver em execução no computador, será capaz de determinar se outros utilizadores foram conectados ao computador ou se o *software* estava em execução, o que permitiria o acesso ao computador pela *internet*.

Finalmente, no que respeita aos *instant messengers*, em alguns casos as mensagens são apagadas automaticamente algum (curto) tempo depois do envio, o que obriga a que, a serem apreendidas, tenham de o ser no momento da pesquisa. Também nestes casos, será impossível não tomar conhecimento, ainda que em pequena medida, dessa conversa. Quanto aos *chats online*, em caso de pesquisa de um sistema informático em que esteja aberta uma conversa reservada, a mesma terá de ser apreendida antes de ser desligado o sistema, sob pena de esta se perder. Igualmente neste caso será impossível não tomar conhecimento, ainda que em pequena medida, dessa conversa.

Em todas estas situações, exigir o prévio conhecimento pelo juiz significaria, na prática, impedir a apreensão desses dados, o que constituiria uma interpretação contra a CCiber e o âmbito de apreensão de dados que Portugal, como Estado-parte, deve assegurar na sua legislação.

Na apreensão de correspondência, a obrigatoriedade de ser o juiz o primeiro a tomar conhecimento do conteúdo da correspondência visa *assegurar que o conteúdo da correspondência estava efectivamente nela contida*. Não é para impedir que outros que não o juiz tomem conhecimento do conteúdo dessa correspondência em caso de irrelevância probatória: se assim fosse, a decisão do juiz de juntar ao processo ou devolver deveria ser irrecorrível. Porém, como isso não está assim prescrito nem no artigo 179.º nem no artigo 400.º do CPP, tal decisão é recorrível[46]. Ora, sendo admissível o recurso dessa decisão, é imprescindível que o Ministério Público tome conhecimento do conteúdo da correspondência para que possa fundamentar devidamente junto do tribunal superior o seu grande interesse para a descoberta da verdade ou para a prova. Sem acesso ao seu conteúdo, este recurso seria uma ficção[47], não sendo sequer possível motivá-lo em conformidade com as exigências do

[45] Exemplos retirados do *Electronic Evidence Guide - A basic guide for police officers, prosecutors and judges*, v. 2.0, elaborado pela Cybercrime Division - Directorate General of Human Rights and Rule of Law, do Conselho da Europa, 2017, p. 147.
[46] Assim, PAULO PINTO DE ALBUQUERQUE, ob. cit., p. 494.
[47] Deste modo, afiguram-se-nos completamente insustentadas práticas de alguns juízes de instrução que, para as mensagens de correio electrónico ou semelhantes, aplicam integralmente o regime do artigo 179.º do CPP e depois

artigo 412.º do CPP. Se a protecção fosse devida ao conteúdo da própria correspondência, deveria manter-se sempre, mesmo depois da abertura – e é consensual que tal não sucede, não se aplicando o regime do artigo 179.º à correspondência já aberta, como vimos.

Ora, tal não faz sentido na correspondência electrónica e semelhante: esta não está fechada, nem é alterável[48]. A operação de "desencapsulamento" que é feita por alguns juízes de instrução não é minimamente equiparável à abertura de correspondência corpórea prevista no artigo 179.º do CPP. Dados informáticos "encapsulados" que se supõe serem mensagens de correio electrónico ou semelhantes não são o equivalente a correspondência fechada: antes de mais, porque aquela nunca esteve fechada; depois, porque não visa (nem consegue) assegurar a integridade do invólucro; finalmente, porque por si não significa tomar conhecimento do conteúdo das mensagens[49].

Deste modo, não há nenhuma real garantia (v.g., para a privacidade) no conhecimento das mensagens de correio electrónico ou semelhantes ser em primeiro lugar do juiz: tal não pode impedir o Ministério Público de, depois, a essas mensagens ter acesso, nomeadamente para poder recorrer da decisão do juiz de não apreensão. *A garantia está apenas na decisão de apreensão/não apreensão e essa não é minimamente afectada pelo conhecimento prévio pelo Ministério Público do conteúdo das mensagens*.

iv. Acusatório e competências do juiz de instrução

Para o fim deixámos o argumento que se nos afigura mais importante: a necessidade de proceder à interpretação do artigo 17.º da LCC em conformidade com a estrutura acusatória do processo, consagrada no artigo 32.º, n.º 5, da CRP, o que significa, na fase de inquérito, respeitar a função do Ministério Público como titular do inquérito e do juiz de instrução como juiz de garantias.

impedem o Ministério Público de tomar conhecimento das mensagens que não seleccionaram, assim assumindo a direcção do inquérito e criando um regime de segredo que deixa de fora o Ministério Público!

[48] Cfr., *supra*, a exigência de certificação digital de que a cópia é absolutamente igual ao original, não tendo nem mais, nem menos *bits*, o que pode ser feito por diversas formas técnicas, nomeadamente por *hashing*. Ainda que tenha existido alteração, o juiz de instrução não será capaz de a detectar (por ser necessário conhecimentos e ferramentas informáticas de que não dispõe), contrariamente ao que sucede com o correio corpóreo, em que isso pode ser detectável com a mera observação do invólucro.

[49] Aliás, quem defende que o juiz deve ser o primeiro a tomar conhecimento do conteúdo das mensagens, tem então, em coerência e sob pena de invalidade, de fazê-lo relativamente a *todas* elas: não basta proceder ao "desencapsulamento", pois tal não significa tomar conhecimento do seu conteúdo, nem tão pouco fazê-lo por amostragem aleatória ou através de pesquisa por palavras-chave. Qualquer uma das mensagens/comunicações não lidas pode ser de extrema relevância para a prova. O facto de, hoje, com elevadíssima probabilidade, qualquer pessoa humana ter na(s) sua(s) conta(s) de correio electrónico milhares de mensagens e, nos seus programas de *instant messaging*, dezenas ou centenas de históricos de comunicações, e de, em estruturas complexas, como grandes sociedades comerciais, tais números poderem ascender aos milhões, não pode constituir fundamento para o juiz se furtar àquela que diz ser função essencial à protecção de direitos fundamentais. É certo que existem ferramentas informáticas utilizadas internacionalmente para análise de grandes quantidades de dados, e.g. mensagens de correio electrónico, de que dispõem algumas polícias de investigação e o Ministério Público, que muito facilitam essa tarefa. Precisamente, porque, como veremos infra, essa análise e selecção é matéria de investigação criminal e não do imparcial juiz das liberdades.

De forma muito simplista, é possível dizer que existem dois grandes modelos de processo penal[50], ainda que, dentro deles, cada país tenha as suas particularidades, que em nenhum exista qualquer modelo em estado puro e que desde há muito que há uma gradual aproximação entre eles. No modelo inquisitório, quem dirige a investigação e acusa é o juiz (nessas vestes chamado de instrução); no acusatório, há separação entre quem acusa e quem julga. Dentro deste, há dois grandes grupos: um em que quem dirige a actividade de investigação criminal é a polícia, outro em que tal é competência do Ministério Público. Na fase de investigação, os juízes são "apenas" juízes de liberdades e garantias.

O sistema português é o acusatório. Como referem GOMES CANOTILHO e VITAL MOREIRA[51], "trata-se de uma garantia essencial do julgamento independente e imparcial. Cabe ao tribunal julgar os factos constantes da acusação e *não conduzir oficiosamente a investigação da responsabilidade penal do arguido (princípio do inquisitório)*. A «densificação» semântica da estrutura acusatória faz-se através da articulação de uma dimensão material (fases do processo) com uma dimensão orgânico-subjectiva (entidades competentes). Estrutura acusatória significa, no plano material, a distinção entre instrução, acusação e julgamento; no plano subjectivo, significa a diferenciação entre juiz de instrução (órgão de instrução) e juiz julgador (órgão julgador) e entre ambos e órgão acusador.".

Efectivamente, para que possa verdadeiramente haver respeito pelos direitos fundamentais dos envolvidos, que o processo conduza a real justiça, é necessário haver separação entre acção e jurisdição. Onde se jogam direitos e liberdade, é imprescindível distanciamento entre quem age e quem julga: quem investiga e acusa não deve julgar; quem julga, não deve investigar, nem ter qualquer intervenção activa na acusação. É condição de um julgamento isento e imparcial que haja distinção entre órgão julgador e órgão acusador. A actuação judicial imparcial exige impulso exterior. O desdobramento funcional do poder punitivo do Estado entre acção e jurisdição é em si uma limitação ao arbítrio. Não por acaso, historicamente, a atribuição de funções ao Ministério Público na acção penal surgiu como limite ao poder absoluto do juiz, que chegou a desempenhar todas as funções no processo penal. Separar para haver controlo recíproco. Para salvaguardar o estatuto de juiz de garante das liberdades, tem de haver repartição de competências entre juiz e Ministério Público, não apenas entre juiz de julgamento e juiz de instrução[52].

Durante o inquérito, o juiz de instrução deve ser apenas juiz de liberdades e garantias: juiz de controlo, não de iniciativa. Deve ser garante dos direitos do visado pela investigação e controlador da actividade do Ministério Público e das polícias criminais que o coadjuvam, não tendo nem devendo por isso ter qualquer empenho nos interesses em conflito, não tomando parte activa na investigação, não dominando o seu impulso, o seu objecto ou o seu resultado.

[50] Como o julgamento cabe sempre ao juiz, a diferença está apenas na titularidade do exercício da acção penal – quem a impulsiona – e, assim, estes modelos são, na sua raiz, modelos de direcção da investigação criminal.
[51] Ob. cit, p. 522.
[52] ANABELA MIRANDA RODRIGUES, "As relações entre o ministério público e o juiz de instrução criminal ou a matriz de um processo penal europeu". in *Que Futuro para o Direito Processual Penal*, Coimbra Editora, simpósio de homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do CPP português. Coord. Mário Monte, Maria Calheiros, Fernando Conde Monteiro, Flávia Loureiro. EDUM. Coimbra: Coimbra editora, 2009, p. 718.

O juiz não pode, ao mesmo tempo, representar o interesse público na repressão criminal e ser um terceiro imparcial, pois são interesses absolutamente incompatíveis. COMO ANABELA MIRANDA RODRIGUES bem adverte, "chamado cada vez mais à boca de cena – num processo crescentemente complexo e onde o conflito verdade/direitos fundamentais se exacerba –, correlativamente exige-se-lhe que se alheie da investigação do caso e da dialética do processo."[53]. Porém, salienta a mesma Autora, "o n.º 4 do artigo 32.º da CRP prossegue a tutela de defesa dos direitos do cidadão no processo criminal e, nessa exacta medida, determina o monopólio pelo juiz da instrução, juiz-garante dos direitos fundamentais dos cidadãos («reserva do juiz»)", "(…) Intervenção do juiz que vale — e só vale — no âmbito do núcleo da garantia constitucional.". Ou seja, concluímos nós, intervenção que apenas deve acontecer na estrita medida do necessário para protecção efectiva dos direitos, liberdades e garantias dos cidadãos, mas não mais do que isso, sob pena de violação do acusatório e da imparcialidade do próprio juiz de instrução.

Este aspecto é salientado, de forma impressiva, pelo Tribunal Constitucional no acórdão 234/11, onde se lê (realces nossos):

> "(…) o disposto no artigo 32.º, n.º 5, da Constituição, quanto aos actos processuais que pudessem ofender direitos fundamentais de qualquer pessoa, também exigiu a supervisão de um juiz, não só pelo seu estatuto de independência, mas também pela sua *distância relativamente à actividade investigatória*.
> A existir, pois, uma reserva ao Ministério Público na direcção da investigação preliminar, ela tem necessariamente de permitir a intervenção do Juiz de Instrução Criminal, nesta fase, em todos os actos instrutórios que possam afectar negativamente direitos fundamentais, de modo a cumprir-se a exigência contida no artigo 32.º, n.º 5, da Constituição. Nesse domínio, existe uma reserva de juiz (…) que comprime a alegada reserva do Ministério Público na direcção do inquérito, *até onde se revele necessária para protecção efectiva dos direitos, liberdades e garantias dos cidadãos*."

Desde o primeiro momento, questionando-se a conformidade constitucional da direcção do inquérito pelo Ministério Público, muitas vezes o Tribunal Constitucional tem sido chamado a pronunciar-se sobre a estrutura acusatória do processo e a repartição de competência entre o juiz de instrução e o Ministério Público durante o inquérito; a necessidade de assegurar a imparcialidade do juiz de instrução e a relevância que, para esse aspecto, reside na própria aparência; a necessidade de impulso do Ministério Público. Desses, salientamos os seguintes, transcrevendo os excertos mais relevantes para o que ora nos ocupa (realces nossos).

No acórdão 129/07:

> "A verdade, porém, é que a imparcialidade dos tribunais é uma exigência não apenas contida no artigo 32º da Constituição, mas uma decorrência do Estado de direito democrático (artigo 2º), na medida em que se inscreve na garantia universal de defesa

[53] "A jurisprudência constitucional portuguesa e a reserva de juiz nas fases anteriores ao julgamento ou a matriz basicamente acusatória do processo penal", in *XXV Anos de Jurisprudência Constitucional Portuguesa, Colóquio Comemorativo do XXV Aniversário do Tribunal Constitucional*, Coimbra: Coimbra Editora, 2009, p. 50.

> dos direitos e interesses legalmente protegidos, através de um órgão de soberania com competência para administrar a justiça (artigo 202º n.º 1 Constituição). Ora, neste dever genérico de imparcialidade do tribunal inclui-se uma exigência de não suspeição subjectiva do juiz; *a actividade do juiz não pode apresentar-se contaminada por circunstâncias geradoras de desconfiança quanto à sua imparcialidade*.
> Todavia, do citado artigo 32º retira-se, para além disto, uma *exigência de imparcialidade objectiva do tribunal*, decorrente da estrutura acusatória do processo penal, circunstância que *impede que o juiz do julgamento esteja envolvido na actividade instrutória, quer carreando para os autos elementos de prova susceptíveis de serem utilizados pela acusação, quer envolvendo-se em actos que possam significar dirigir a investigação*. Esta exigência de imparcialidade objectiva do juiz justifica-se do ponto de vista das garantias da defesa, é certo, mas igualmente pela necessidade de proporcionar ao juiz as condições de isenção requeridas pelo exercício das suas funções.".

No acórdão 581/2000:

> "Se das garantias de defesa se retira o dever de imparcialidade da entidade que conduz e dirige o inquérito e formula a acusação, delas também se retira a imparcialidade e independência da entidade que, antes do julgamento, procede à aplicação de medidas restritivas de direitos fundamentais ou autoriza a prática de actos instrutórios que se prendem directamente com direitos fundamentais."
> E cita depois N. Gonzalez-Cuellar Serrano (*Proporcionalidad y Derechos Fundamentales en el Processo Penal*, Madrid, 1990, p. 132): "[...] ao serem estes últimos [os juízes de instrução] competentes para aplicar as medidas restritivas dos direitos fundamentais antes do julgamento, carecerão da imparcialidade que, em nossa opinião, deve também mostrar-se para a adopção de decisões dessa natureza. Pelo contrário, *se aquelas medidas limitativas de direitos forem solicitadas pelo Ministério Público, o juiz, desprovido de funções de investigação e, por isso, de ânimo persecutório, alcançará a objectividade exigível para decidir sem preconceitos*".

A interpretação conjugada do artigo 17.º da LCC e do artigo 179.º do CPP no sentido de aí fundar uma norma com o sentido de que é o juiz de instrução que, no inquérito, em primeiro lugar toma conhecimento das mensagens de correio electrónico ou semelhantes e que é ele que, oficiosamente, procede à selecção daquelas que são de grande interesse para a descoberta da verdade ou para a prova, para além de não se traduzir em qualquer real garantia, viola a estrutura acusatória do processo, pois essa é matéria essencial à direcção do inquérito e à definição do seu objecto, assim comprometendo a posição de imparcial juiz das liberdades.

O juiz de instrução não pode ter qualquer "influência" ou "manipulação" sobre a definição do objecto do inquérito[54]; deve ser alheio à definição da estratégia de investigação do Ministério Público e OPC's, devendo actuar apenas no campo da admissibilidade legal das intervenções

[54] FIGUEIREDO DIAS, "Sobre os sujeitos processuais no novo Código de Processo Penal", in. Jornadas de Direito Processual Pena – O Novo CPP, Coimbra: Almedina, p. 16 e p. 33.

requeridas[55], sendo por isso sua obrigação, "uma vez verificados os pressupostos formais de procedência, deferir o requerido pelo Ministério Público"[56], "não podendo, em caso algum, examinar a utilidade da medida requerida"[57]. "A competência do juiz de instrução durante a fase processual presidida pelo Ministério Público, sempre que estejam em causa actos que interferem com direitos fundamentais e outras matérias que a lei reserve ao juiz, obedece a um quadro de intervenção tipificada e provocada, pois a magistratura judicial por natureza não actua *ex oficio* em processos de que não é titular", devendo acentuar-se que este princípio da inoficiosidade "não deriva de um preconceito histórico, mas de um modelo garantista em que se condiciona a intervenção do único órgão com poderes em áreas fundamentais de direitos liberdades e garantias à intervenção prévia de uma outra entidade."[58].

A interpretação que criticamos coloca no juiz de instrução a competência para verdadeiramente investigar os factos noticiados e impor ao Ministério Público a utilização de concretos meios de prova: analisar cada uma das comunicações, conjugá-las entre si, relacioná-las com os demais meios de prova existentes, aferir da sua relevância para o que demais se planeia fazer, tudo elevado a uma escala que, em processos complexos, cada vez mais frequentes, não será exequível sem meios técnico-informáticos adequados.

Exigir que seja o juiz a oficiosamente seleccionar as mensagens relevantes é tão fundamentado como seria exigir que o Ministério Público apresentasse ao juiz de instrução uma lista de casas onde, em abstracto, pudessem existir objectos relacionados com um crime ou que pudessem servir de prova, ou uma lista de pessoas que, em abstracto, pudessem ter conhecimento dos factos, e ser o juiz de instrução a ordenar em quais dessas casas se fariam buscas e quais dessas pessoas seriam inquiridas como testemunhas, a realizar tais diligências e a apresentar depois ao Ministério Público os resultados que considerasse relevantes para a prova.

Tal interpretação é um regresso ao sistema que vigorou para as escutas telefónicas na versão original do CPP – que não permitia aos OPC's e ao Ministério Público tomarem conhecimento do seu conteúdo antes do juiz de instrução –, que, após críticas, veio a ser modificado, primeiro na reforma de 1998 e depois na de 2007.

Por tudo o que fica exposto, nessa interpretação, o artigo 17.º da LCC conteria uma norma desconforme ao n.º 5 do artigo 32.º da CRP. Ora, nos feitos submetidos a julgamento não podem os tribunais aplicar normas que infrinjam o disposto na Constituição ou os princípios nela consignados – artigo 204.º da Lei Fundamental. Em consequência, deve proceder-se a uma interpretação conforme à Constituição[59], que é aquela que antes apresentámos.

[55] Assim, PAULO DÁ MESQUITA, *Direcção do Inquérito Penal e Garantia Judiciária*, 2003, p. 176.
[56] FIGUEIREDO DIAS, "Do princípio da "objectividade" ao princípio da "lealdade" do comportamento do ministério público no processo penal", Revista de Legislação e Jurisprudência, ano 128, p. 351.
[57] CLAUS ROXIN, apud PAULO DÁ MESQUITA, ob. cit., p. 176, nota 53.
[58] PAULO DÁ MESQUITA, ob. cit., p. 174-175.
[59] Refere JORGE MIRANDA que "(...) cada norma legal não tem somente de captada no conjunto das normas da mesma lei e no conjunto da ordem legislativa; tem outrossim de se considerar no contexto da ordem constitucional". Precisando depois que "A interpretação conforme à Constituição não consiste tanto em escolher, entre vários sentidos possíveis e normais de qualquer preceito, o que seja mais conforme com a Constituição quanto em discernir no limite – na fronteira da inconstitucionalidade – um sentido que, conquanto não aparente ou não decorrente de outros elementos de interpretação, é o sentido necessário e o que se torna possível por virtude da

Consentindo o teor verbal da norma interpretanda dois sentidos – um desconforme e outro conforme à Constituição –, o intérprete deve adoptar este último[60].

VII. PRAZOS PARA APRESENTAÇÃO AO JUIZ

Prescreve o artigo 16.º, n.º 4, da LCC que "As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.". Como vimos já[61], esse prazo inicia-se com a conclusão da pesquisa e elaboração do respectivo auto (se em cumprimento de ordem de autoridade judiciária) ou relatório (na sua ausência).

No inquérito, o OPC apresentará ao Ministério Público, em 72 horas, os dados apreendidos (distinguindo aqueles susceptíveis de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro) e, em suporte autónomo, as mensagens de correio electrónico ou semelhantes cuja apreensão considera de grande interesse para a descoberta da verdade ou para a prova. O Ministério Público deverá, nesse prazo, proceder à validação do já apreendido (se validamente apreendido, naturalmente) – artigo 16.º, n.º 4. Para além disso, deverá apresentar ao juiz de instrução quer os dados já apreendidos susceptíveis de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, requerendo fundamentadamente a sua admissão probatória pela sua relevância (artigo 16.º, n.º 3), quer, noutro suporte, as mensagens de correio electrónico ou semelhantes, requerendo fundamentadamente a apreensão daqueles que considera de grande interesse para a descoberta da verdade ou para a prova (artigo 17.º).

Não havendo prazo expressamente previsto na lei para esta apresentação ao juiz, afigura-se-nos que haverá que aplicar o prazo supletivo de 10 dias previsto no artigo 105.º, n.º 1, do CPP.

VIII. MENSAGENS DE CORREIO ELECTRÓNICO OU SEMELHANTES NÃO APREENDIDAS

Antes de terminar, deixamos uma breve nota sobre o que fazer às mensagens de correio electrónico ou semelhantes que não sejam apreendidas por não serem de grande interesse para a descoberta da verdade ou para a prova.

Os dados informáticos a que se aplica o artigo 17.º são dados armazenados que poderiam ter sido interceptados, em tempo real, através dos meios de obtenção de prova previstos nos artigos 187.º e 188.º do CPP (*SMS, EMS* e *MMS*) ou no artigo 18.º da LCC (e.g., mensagens de correio electrónico e *instant messaging*). Assim, quanto ao regime da destruição/devolução, sendo o artigo 17.º omisso e não oferecendo o artigo 179.º do CPP, como vimos, resposta

força conformadora da Lei Fundamental." - *Manual de Direito Constitucional*, Vol. I, Tomo I, Coimbra: Coimbra Editora, 2014, p. 233.

[60] Neste sentido, cfr. os acórdãos do Tribunal Constitucional n.ºs 266/92 e 364/94.

[61] Cfr. nota 4.

satisfatória, deve aplicar-se o regime do artigo 188.º, n.º 6, deste código, *ex vi* do artigo 28.º da LCC. Sendo os dados da mesma natureza, deve o regime de conservação ser o mesmo.

IX. CONCLUSÕES

Sendo cada vez mais relevante a utilização como meio de prova no processo penal das mensagens de correio electrónico e de natureza semelhante que são encontradas apreendidas em sistemas informáticos, é matéria onde se exige, com particular acuidade, a protecção de direitos fundamentais. Ainda que não exactamente do direito à inviolabilidade da correspondência e das telecomunicações, mas sempre do direito ao desenvolvimento da personalidade e do direito à reserva da intimidade da vida privada.

Para essa apreensão, o legislador deveria ter criado um regime autónomo e auto-suficiente, com repartição equilibrada de competências entre o Ministério Público e o juiz de instrução, a este reservando o estritamente necessário à garantia de direitos dos visados, adequado às especificidades técnicas das comunicações electrónicas, muito diferentes da correspondência corpórea, e à estrutura acusatória do processo penal, o que, pelo menos de forma satisfatória, não fez no artigo 17.º da LCC.

No campo de aplicação deste artigo estão as mensagens de correio electrónico, transmitidas através da *internet* ou em *intranets*, e comunicações de natureza semelhante, quer as feitas através de serviço telefónico (SMS, EMS e MMS), quer através da internet (como por *instant messengers* ou *chatrooms*), independentemente do seu conteúdo, de estarem nos servidores dos ISP ou já descarregadas nos sistemas dos utilizadores e de terem ou não sido abertas/lidas.

O artigo 17.º da LCC determina a correspondente aplicação do regime de apreensão de correspondência do CPP, não a aplicação integral. Esta só deve ser feita naquilo que não contrariar o já previsto na própria LCC; a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC. Nomeadamente, não será de aplicar nem o âmbito objectivo nem o subjectivo do artigo 179.º do CPP, e, no que respeita aos procedimentos, no inquérito é ao Ministério Público que compete proceder à análise e selecção das mensagens com grande interesse para a descoberta da verdade ou para a prova, que depois apresentará ao juiz em suporte autónomo juntamente com requerimento fundamentado, após o que o juiz apreciará, tomando conhecimento do seu conteúdo, e decidirá autorizar ou não autorizar a apreensão formal.

Esta a interpretação mais conforme à letra da lei, que maior coerência confere ao complexo normativo de tutela de direitos em matéria de dados de comunicações electrónicas, que respeita as diferenças de natureza entre o correio corpóreo e correio electrónico ou semelhante, e, finalmente, a estrutura acusatória do nosso processo penal.

6.

Métodos ocultos de investigação criminal em ambiente digital

David Silva Ramalho

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6. MÉTODOS OCULTOS DE INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL[1]

David Silva Ramalho*

Apresentação *Power Point*
Vídeo

Apresentação *Power Point*

[1] Apresentação decorrida na ação de formação "Temas de Direito Penal e Processual Penal", no CEJ, no dia 10 de março de 2017.
* Advogado.

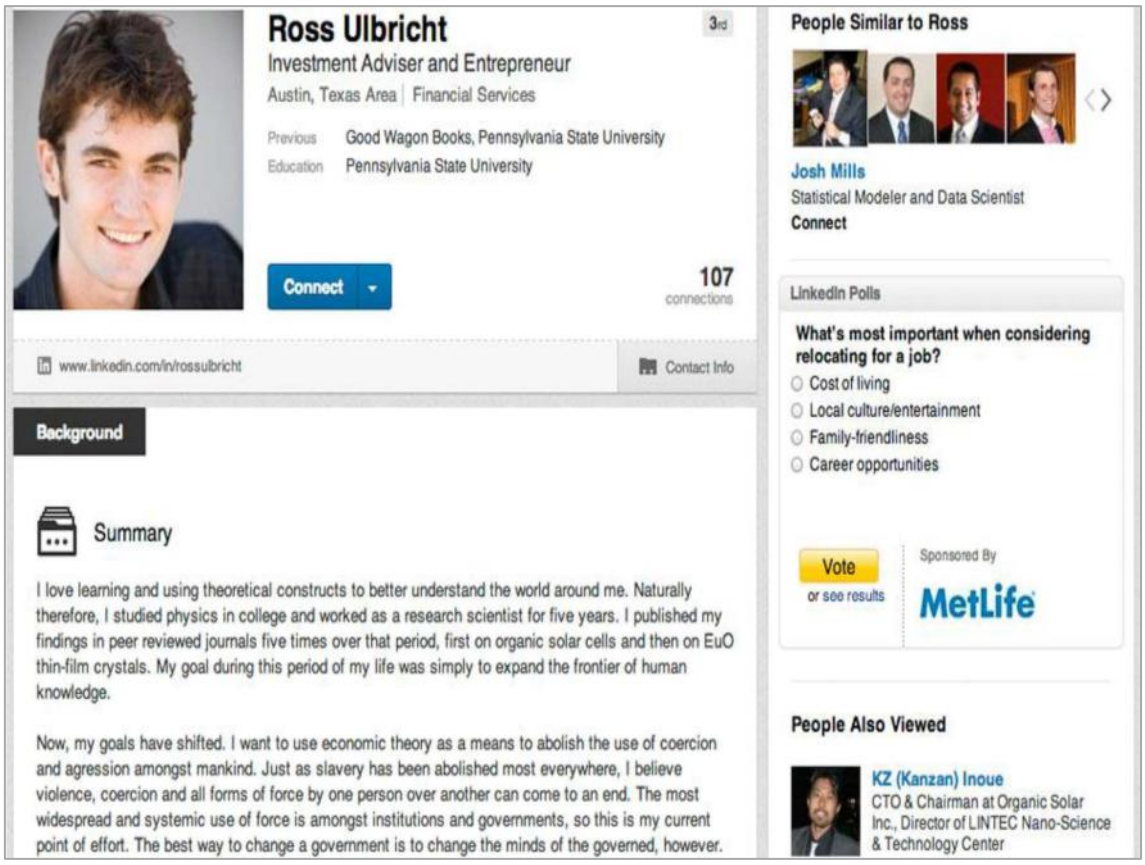
Métodos ocultos de investigação criminal em ambiente digital

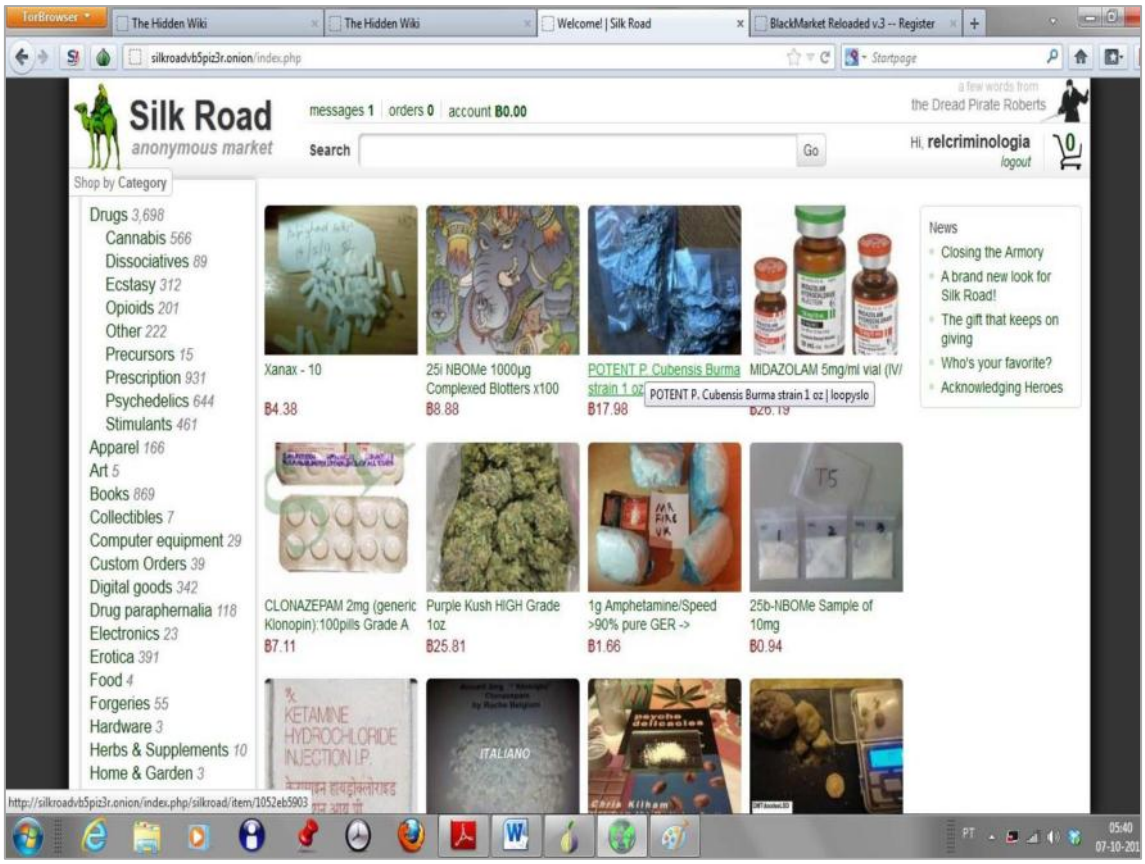
1. Dificuldades da investigação criminal em ambiente digital.
2. O recurso a métodos ocultos de investigação criminal.
3. O acesso oculto a dados informáticos armazenados.
4. As acções encobertas em ambiente digital.
5. *Hacking* e o uso de *malware*

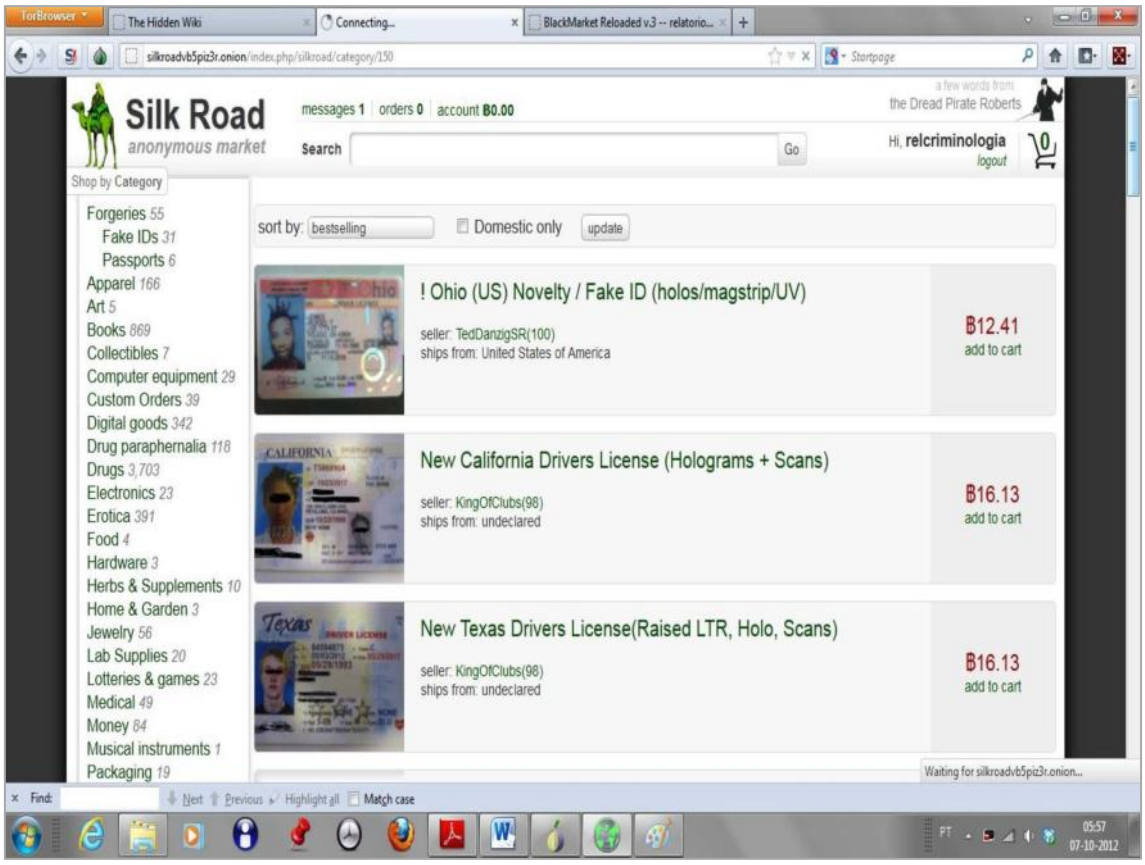
CENTRO DE ESTUDOS JUDICIÁRIOS

1. Dificuldades da investigação criminal em ambiente digital

CENTRO DE ESTUDOS JUDICIÁRIOS


Ross Ulbricht
3rd
Investment Adviser and Entrepreneur
Austin, Texas Area | Financial Services
Previous Good Wagon Books, Pennsylvania State University
Education Pennsylvania State University
Connect
107
connections
www.linkedin.com/in/rossulbricht
Contact Info
Background
Summary
I love learning and using theoretical constructs to better understand the world around me. Naturally therefore, I studied physics in college and worked as a research scientist for five years. I published my findings in peer reviewed journals five times over that period, first on organic solar cells and then on EuO thin-film crystals. My goal during this period of my life was simply to expand the frontier of human knowledge.
Now, my goals have shifted. I want to use economic theory as a means to abolish the use of coercion and agression amongst mankind. Just as slavery has been abolished most everywhere, I believe violence, coercion and all forms of force by one person over another can come to an end. The most widespread and systemic use of force is amongst institutions and governments, so this is my current point of effort. The best way to change a government is to change the minds of the governed, however.
People Similar to Ross
Josh Mills
Statistical Modeler and Data Scientist
Connect
LinkedIn Polls
What's most important when considering relocating for a job?
Cost of living
Local culture/entertainment
Family-friendliness
Career opportunities
Vote
or see results
Sponsored By
MetLife
People Also Viewed
KZ (Kanzan) Inoue
CTO & Chairman at Organic Solar Inc., Director of LINTEC Nano-Science & Technology Center


TorBrowser
The Hidden Wiki
The Hidden Wiki
Welcome! | Silk Road
BlackMarket Reloaded v.3 -- Register
silkroadvb5piz3r.onion/index.php
Silk Road
anonymous market
messages 1 | orders 0 | account B0.00
Search
Go
a few words from the Dread Pirate Roberts
Hi, relcriminologia
logout
Shop by Category
Drugs 3,698
Cannabis 566
Dissociatives 89
Ecstasy 312
Opioids 201
Other 222
Precursors 15
Prescription 931
Psychedelics 644
Stimulants 461
Apparel 166
Art 5
Books 869
Collectibles 7
Computer equipment 29
Custom Orders 39
Digital goods 342
Drug paraphernalia 118
Electronics 23
Erotica 391
Food 4
Forgeries 55
Hardware 3
Herbs & Supplements 10
Home & Garden 3
Xanax - 10
B4.38
25i NBOMe 1000µg Complexed Blotters x100
B8.88
POTENT P. Cubensis Burma strain 1 oz
B17.98
MIDAZOLAM 5mg/ml vial (IV/
CLONAZEPAM 2mg (generic Klonopin):100pills Grade A
B7.11
Purple Kush HIGH Grade 1oz
B25.81
1g Amphetamine/Speed >90% pure GER ->
B1.66
25b-NBOMe Sample of 10mg
B0.94
News
Closing the Armory
A brand new look for Silk Road!
The gift that keeps on giving
Who's your favorite?
Acknowledging Heroes
KETAMINE HYDROCHLORIDE INJECTION I.P.
ITALIANO
http://silkroadvb5piz3r.onion/index.php/silkroad/item/1052eb5903



1.1. Dificuldades na identificação do agente do crime

- Anonimizadores (*proxies*, TOR, *Freedom Hosting*);
- Moedas virtuais (*bitcoins* e *altcoins*);
- Conservação de dados de tráfego *(data retention);*
- Aspectos jurisdicionais

CENTRO DE ESTUDOS JUDICIÁRIOS

1.2. Dificuldades na descoberta e valoração da prova

- Cifragem de dados;
- Cifragem do disco;
- Alteração de *metadata,* como data de criação (*Timestomp*);
- Ataques contra perícias forenses.

CENTRO DE ESTUDOS JUDICIÁRIOS

2. O recurso a métodos ocultos de investigação criminal

CENTRO DE ESTUDOS JUDICIÁRIOS

2.1. Características

- Métodos ocultados do visado;
- Um imperativo de eficácia;
- Neutralizam alguns dos seus direitos processuais (e.g. não auto-incriminação ou direito a recusar prestar testemunho);
- São abrangentes (incluem terceiros e não se limitam ao momento do facto);
- Ignoram a intimidade e fiabilidade da comunicação.
- O centro do processo desloca-se para o inquérito

CENTRO DE ESTUDOS JUDICIÁRIOS

2.1. Características

- Métodos ocultados do visado;
- Um imperativo de eficácia;
- Neutralizam alguns dos seus direitos processuais (e.g. não auto-incriminação ou direito a recusar prestar testemunho);
- São abrangentes (incluem terceiros e não se limitam ao momento do facto);
- Ignoram a intimidade e fiabilidade da comunicação.
- O centro do processo desloca-se para o inquérito

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Métodos ocultos atípicos?

    1 – Delimitação positiva: subsidiariedade da prova atípica à típica;

    2 – Existência de limites expressos na lei e CRP

    3 – Aptidão para restringir direitos fundamentais

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Segurança jurídica;
  - Prevenção de abuso e arbítrio;
  - Conhecimento pela comunidade dos meios à disposição da investigação;
  - Possibilidade de sindicar a sua legalidade;

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Proibição de analogia ou de argumentos por *maioria de razão* (e.g. acção encoberta e escutas).
    - Diferente de intervenção restritiva legitimada pela norma mas executada com um âmbito mais circunscrito

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - A lei como ponderação *específica*.
  - Não se aplica a novos modos de execução de métodos de obtenção típicos.
  - Necessidade de densidade normativa da habilitação legal, ainda que permitindo uma ponderação concreta.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - Primeiro do legislador, depois do aplicador;
  - **Adequação**: susceptibilidade de o meio permitir a realização eficaz do fim da restrição.
    - Tendencialmente de verificação prática e não legislativa.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - **Necessidade**: Entre os meios à disposição deve ser escolhido aquele que, em concreto, face aos pressupostos da lei e às circunstâncias do caso concreto, se revela necessário, exigível ou indispensável para atingir o fim.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - **Proporcionalidade *stricto sensu***: verificação da *justeza* (ou da justa medida) da medida restritiva.
  - Critério da não desproporcionalidade?
  - Temperado por critérios objectivos: gravidade, força dos indícios, sanção previsível, etc.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da subsidiariedade:
  - No plano extrínseco: prioridade aos métodos *abertos*.
  - No plano intrínseco: o menos grave dos disponíveis;
  - Evitar a cumulação de métodos ocultos.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de juiz:
  - O direito fundamental ao juiz.
  - Um "tigre sem dentes"?
  - Várias excepções.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- A tutela jurídica do ambiente digital:
  - Autonomia ontológica da realidade digital;
  - Localização geográfica, conteúdo, ligação à Internet, extensão a outros sistemas.
  - O direito à integridade e confidencialidade dos sistemas informáticos (BVerfG) ou o direito à não intromissão no ambiente digital (Gonzalez-Cuellar Serrano).

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- Os conhecimentos fortuitos:
  - O problema da dimensão da informação e da existência de um *motor de busca*;
  - Crimes de catálogo vs meios livres;
  - O princípio do limiar da intervenção equivalente ou da intervenção substitutive hipotética e a mudança de fim que justifica o meio.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- O direito a um contraditório qualificado:
  - O carácter técnico e hermético da informação sobre diligências informáticas;
  - A fragilidade da prova digital;
  - A necessidade de relatórios claros e densos.

CENTRO DE ESTUDOS JUDICIÁRIOS

3. O acesso oculto a dados informáticos

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

- As normas da pesquisa estão pensadas para um contexto de busca;
- A pesquisa do artigo 15.º, n.º 5, da Lei do Cibercrime não pode, por natureza, ser oculta;
- Mas e a do 15.º, n.º 1?

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

- A quem se dirige a cópia do despacho imposta pelo artigo 176/1 CPP ex vi 15/6 CPP?
- Quem tem a *disponibilidade* dos dados?
- A aplicação do regime das buscas "com as necessárias adaptações".
- Como preside a AJ à diligência?

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

- Se não for admissível, será que apenas se pode aceder a outro Sistema a partir do 15/5 da LC?
- Obrigação de recorrer à injunção para apresentação ou concessão do acesso a dados?

CENTRO DE ESTUDOS JUDICIÁRIOS

3.2. Outros meios

- A injunção para concessão ou apresentação do acesso a dados.
- A obtenção de dados de tráfego:
  - Problema da eventual impossibilidade de aplicação da Lei n.º 32/2008.

CENTRO DE ESTUDOS JUDICIÁRIOS

4. As acções encobertas

CENTRO DE ESTUDOS JUDICIÁRIOS

4. As acções encobertas

- É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes: [...]

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

- Comparação permanente com as acções encobertas em ambiente físico:
  - O início das acções encobertas *online* (*chats* e *posts* com link de conhecimento reservado; integração pública v. privada, activa v. passiva).
  - As múltiplas personalidades sucedâneas ou simultâneas numa ou mais salas de chat (o agente pode ser o traficante, o comprador, o menor ou o pedófilo – tem de ser regulado).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

- A apropriação da identidade de terceiros (v. caso Silk Road).
- O risco de abusos por parte do agente encoberto (v. Carl Force IV e Shaun Bridges – 250.000,00$ em bitcoins).
- As novas vias de fronteira entre encobrimento e provocação (nomes provocadores ou identidades de ex-participantes).
- O registo integral e passivo de salas públicas.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

- Os terceiros infiltrados, em particular, os terceiros integrados na rede criminosa;
- Pode assumir a figura de agente infiltrado, o indivíduo que cometeu crimes no meio investigado?
  - Pode mas em geral não terá especial interesse;
  - as suas declarações serão sempre prestadas ao abrigo do regime aplicável ao co-arguido (cf. artigo 345.º, n.º 4, do CPP) e nunca ao das testemunhas (cf. artigo 133.º, n.º 1, alínea *a)*), do CPP),
  - Por força do seu estatuto processual, o arguido poderá sempre recusar-se a prestar declarações em sede de julgamento.
  - Pode valer para recolha e registo autónomo de prova

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. Problemas na aplicação da Lei 101/2001

– Identidade fictícia *online* mediante proposta do Director nacional da PJ e atribuída pelo MJ (usernames próprios ou de terceiros)?
  - Mas o mesmo username pode ser utilizado por vários agentes.
  - Questão operacional?
  - O relato do agente encoberto.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. Problemas na aplicação da Lei 101/2001

– A isenção de responsabilidade apenas quanto a actos preparatórios ou em em qualquer forma de comparticipação diversa da instigação e da autoria mediata (a *lógica de comparticipação*).
  - Problemas em *peer-to-peer;*
  - Envio de ficheiros de conteúdo ilícito (analogia com as entregas controladas).
  - É necessária a publicação de regras ou manuais de boas práticas ou afins.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. O regime espanhol (LO 13/2015)

Novo artigo 282.º bis

6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en **comunicaciones mantenidas en canales cerrados de comunicación** con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, **con autorización específica para ello**, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.4. Os *siti civetta*

- Siti civetta: Artigo 14/2 da *Legge* 3 agosto 1998, n. 269, que aprovou a lei contra a exploração da prostituição, da pornografia, do turismo sexual contra crianças, como novas formas de redução à escravidão.
- Criação de websites e gestão de áreas de comunicação como *chats.*

CENTRO DE ESTUDOS JUDICIÁRIOS

5. *Hacking* e o uso de *malware*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- *Malicious + software*

«um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça»

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Logic bombs;
- Spyware
- Rootkits;
- Virus;
- Worms
- Blended threats
- Keyloggers, sniffers, etc

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Permitem:
  - Recolher informação (incluindo credenciais de acesso) para envio a terceiros;
  - Criar *backdoors* (acesso remoto, contornar os mecanismos de autenticação);
  - Instalar mais *malware*;
  - Monitorizar a actividade do utilizador;
  - Activar o *hardware*, como microfones e *webcams*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Processos de instalação:
  - Via suporte físico removível (útil para redes locais);
  - Via *Web browser* (*drive-by downloads*) –Ex. *Magneto* e Freedom Hosting (MAC address e nome de utilizador do administrador do Windows, e, por fim, o IP);
  - Via *download* (*e-mails,* programas, falsas actualizações).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Software vendido a vários Estados, incluindo aos governos do Sudão, da Rússia, das Honduras, do Equador, do Panama e da região do Curdistão.

Após divulgação do código fonte do RCS Galileo, ele começou a ser utilizado por cibercriminosos para infiltrar computadores de terceiros

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Remote Control System Galileo:

- Fácil de utilizar, inclusivamente por quem não seja especialista em tecnologias de informação.
- Em cerca de duas semanas, o agente de investigação está pronto a utilizá-lo.
- *Se os hackers são piratas, a Hacking Team é um corsário - Vaciago*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Funcionalidades do *Galileo:*

- *Intercepção de comunicações*
- *Activação remota de webcams e microfones*
- *Activação das funcionalidades GPS*
- *Instalação de keyloggers*
- *Gravação de comunicações em IM (incluindo Skype)*
- *Screenshots da actividade do utilizador, etc.*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Processo de instalação do *Galileo:*

- Processo de instalação:
- *Via vulnerabilidades do Flash, Word, etc.*
- *Engenharia social*
- *Ocupa menos de 1 MB*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: jurisprudência

Italian Supreme Court of Cassation, Division V, Decision No. 24695, of 14 October 2009

The Italian Supreme Court did not find in the tools any kind of surveillance, based on the assumption that the investigative activity consisted of seizing and copying documents stored on the hard disk of the device used by the accused, and **did not involve any 'flow of communications',** but only 'an operational relationship between the microprocessor and video of the electronic system'.

This definition enabled the Public Prosecutor to avoid seeking a search warrant from the judge in charge of Preliminary Investigations to activate such a kind of tool.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: jurisprudência

Questão foi colocada no plenário do Supremo para resolução do conflito de orientações jurisprudenciais:

Pergunta-se: possível levar a cabo vigilância electrónica entre pessoas presentes através da instalação deste tipo de ferramentas em dispositivos electrónicos portáteis, mesmo em contexto privado, apesar de não identificadas separadamente e mesmo se nenhuma actividade criminosa esteja a decorrer entre eles?

Tribunal admitiu-o em criminalidade muito grave.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: legislação

Nos últimos 4 anos houve 4 tentativas de regulamentar o malware.

As primeiras duas foram alvo de críticas por não serem suficientemente garantísticas.

Encontram-se em discussão duas propostas.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

Artículo 588 septies a. Presupuestos. 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.4. Outras experiências

- **França**: *captation des donées informatiques* 8arts. 706-102-1 a 706-102-9
- **Finlândia**: "instalação de dispositivo, procedimento ou programa num Sistema informático para fins de vigilância técnica" (art. 26.º do capítulo 10 da Lei n.º 806/2011).
- **Holanda**: Nova proposta, alterada em Dezembro de 2015, que prevê o poder de aceder remotamente a sistemas informáticos

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português

- Aplicação do regime das escutas?
- Aplicação do regime das escutas + buscas?
- Aplicação do regime da intercepção de comunicações?
- Extensão prevista no artigo 15.º, n.º 5, da Lei do Cibercrime?

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português

"Sendo necessário **o recurso a meios e dispositivos informáticos** observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações" (art. 19.º, n.º 2, da Lei do Cibercrime).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

a) Adequação aos fins de prevenção e repressão criminais identificados em concreto e proporcionais, quer a essas finalidades, quer à gravidade do crime sob investigação (artigo 3.º, n.º 1, da Lei n.º 101/2001, de 25 de agosto);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

b) Fundadas suspeitas da prática de um dos crimes previstos na Lei do Cibercrime ou de crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras,bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos (artigo 19.º, n.º 1, da Lei do Cibercrime);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

c) A sua utilização apenas pode ocorrer quando houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (artigo 18.º, n.º 2, da Lei do Cibercrime);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

d) A precedência de despacho fundamentado do juiz de instrução, mediante requerimento do Ministério Público (artigo 18.º, n.º 2 da Lei do Cibercrime). Não uma espécie de *deferimento tácito*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

e) A delimitação dos dados que se visa obter, de acordo com as necessidades concretas da investigação (artigo 18.º, n.º 3 da Lei do Cibercrime).

CENTRO DE ESTUDOS JUDICIÁRIOS

Obrigado pela V. atenção!

dsramalho@mlgts.pt

CENTRO DE ESTUDOS JUDICIÁRIOS

Vídeo da apresentação

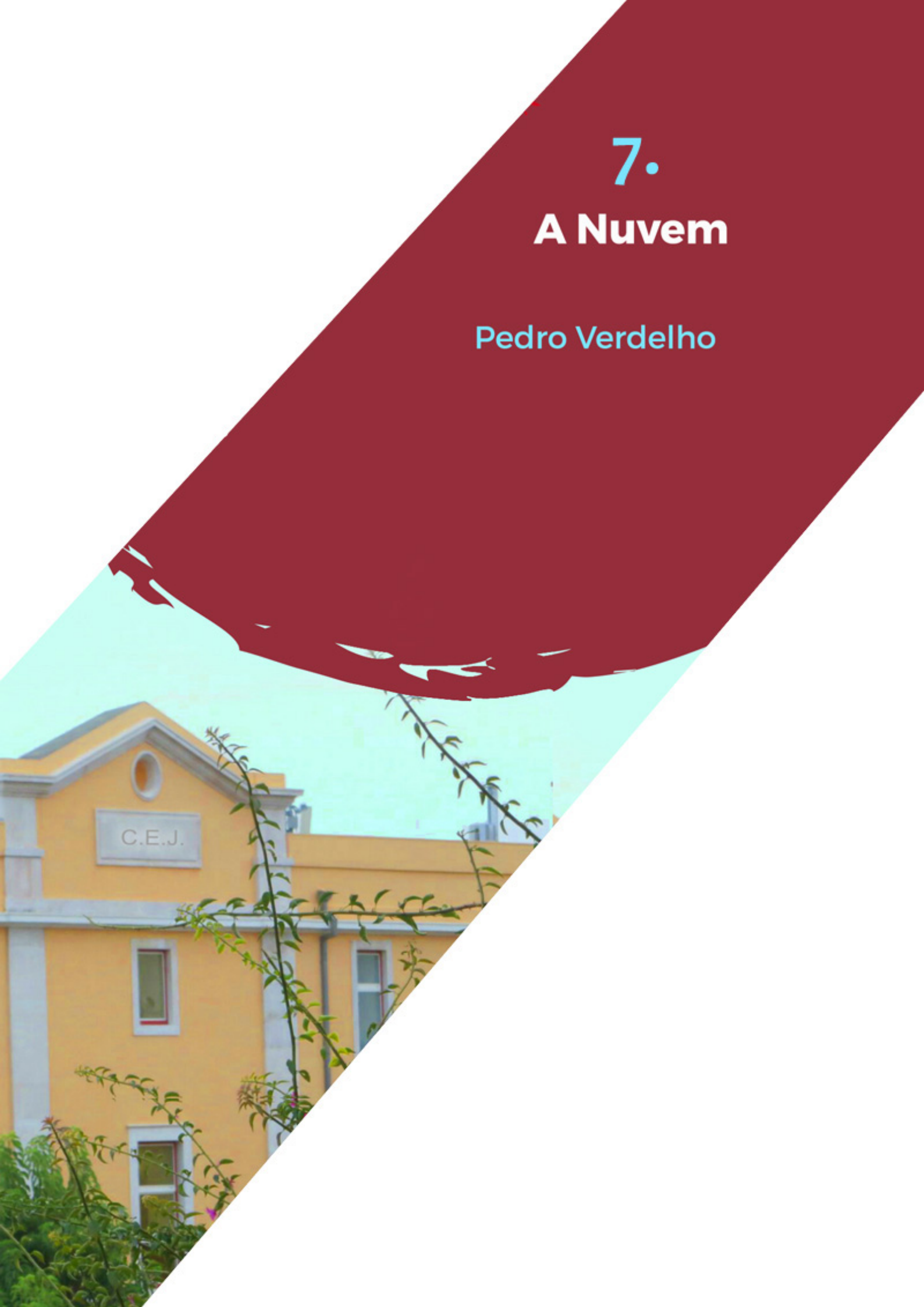
➔ https://educast.fccn.pt/vod/clips/4f7gyvrcg/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

7.

A Nuvem

Pedro Verdelho



CENTRO
DE ESTUDOS
JUDICIÁRIOS

7. A NUVEM[1]

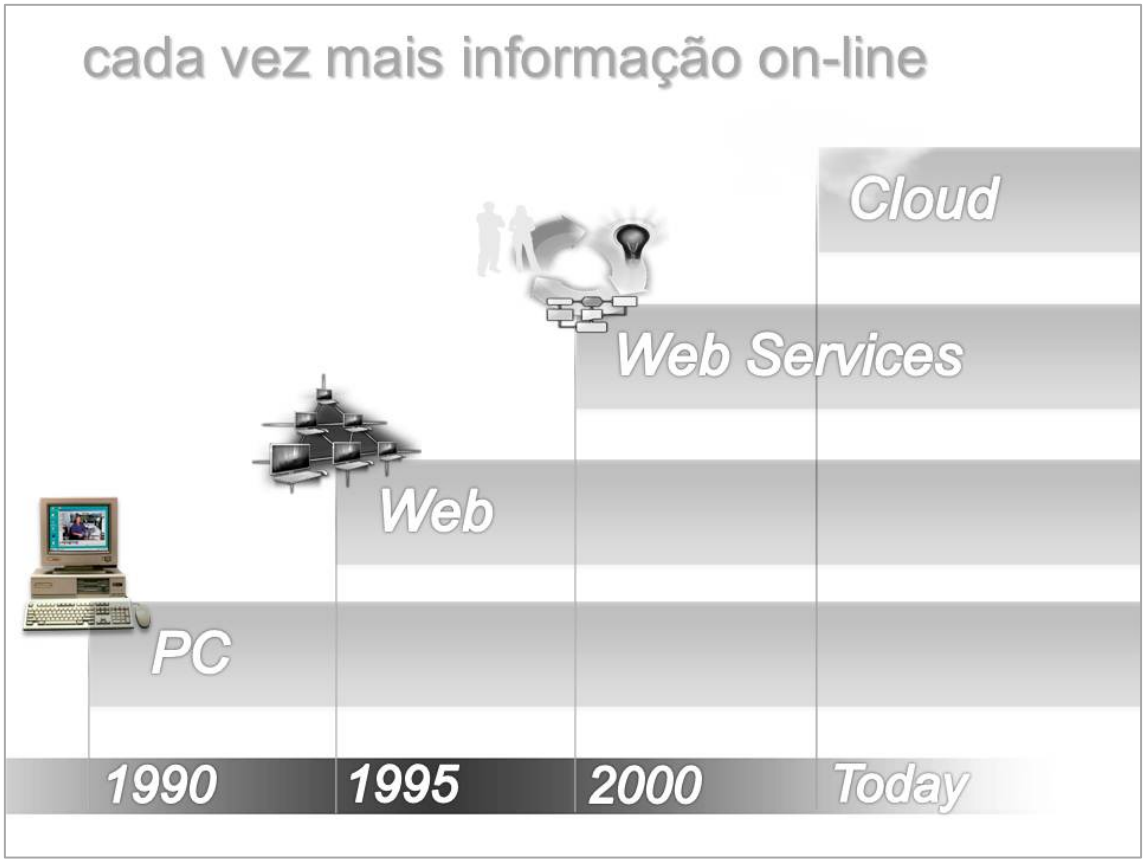
Pedro Verdelho*

Apresentação *Power Point*
Vídeo

Apresentação *Power Point*

[1]Apresentação decorrida na ação de formação "Prova em Direito Penal, cibercriminalidade e prova em ambiente digital", no CEJ, nos dias 7 e 8 de abril de 2016.
* Procurador da República, Coordenador do Gabinete Cibercrime da PGR.


a Internet está
globalmente implantada


cada vez mais informação on-line
Cloud
Web Services
Web
PC
1990
1995
2000
Today

"aqui" é "em lado nenhum"

"aqui" é "em lado nenhum"

- a prova está espalhada a nível global

- a prova está "em lado nenhum"
  - pode estar localmente, em dispostivos
  - mas provavelmente estará também algures no mundo
- necessidade de obter prova fora das nossas próprias fronteiras

- não há alternativa – os crimes já não são apenas "*nacionais*"

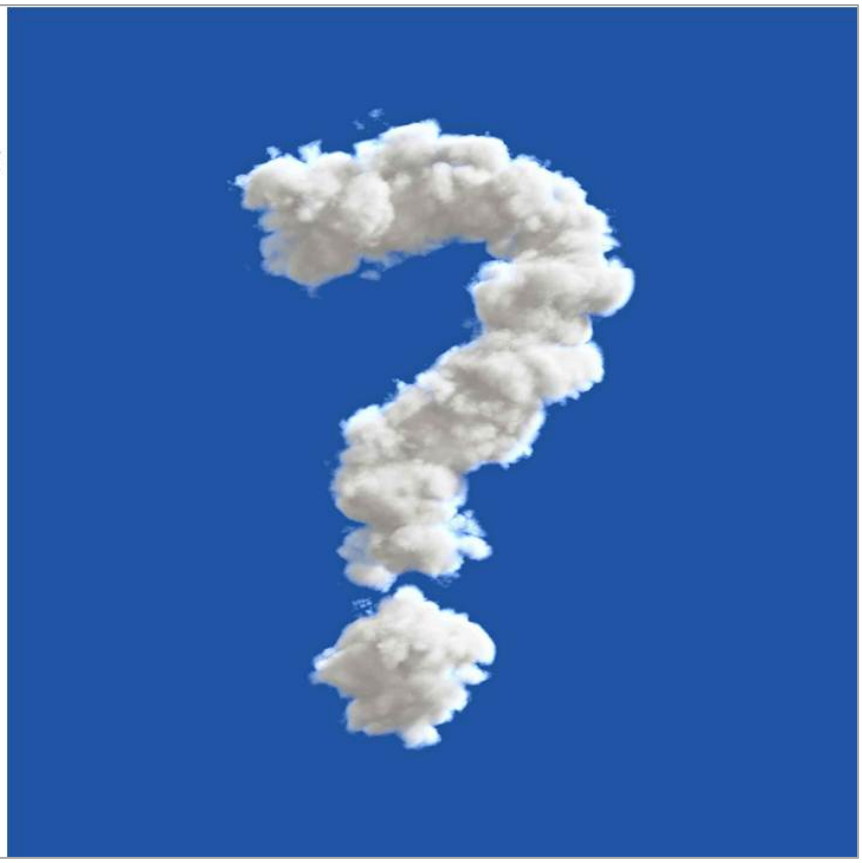
- desafios:
  - identificar o infrator e a dimensão do crime
  - volatilidade da prova eletrónica
  - necessidade de investigações céleres e confidenciais
- as regras processuais têm que adaptar-se para fazer frente a estes desafios

6

prova "digital"/ "electrónica"

- não se circunscreve a casos de cibercrime
- muitos dos crimes modernos (tal como os tradicionais) requerem que se analise prova digital
- é atualmente enorme o volume de prova electrónica

Questões Difíceis:



"questões difíceis:

1 – localização de um crime – onde foi cometido:

- que lei penal substantiva é a aplicável?
- qual é a jurisdição competente (polícia, Ministério Público, juiz)

2 – jurisdição como um limite à obtenção de prova

- investigações trans-fronteiriças – investigações na "cloud" – acesso a dados armazenados na "cloud"

Convenção de Budapeste

Artigo 32º

Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

(…)

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, **se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados**, através deste sistema informático.

- localização desconhecida
- localização múltipla
- localização fora de um Estado Parte

Questões

- localização desconhecida:
- cooperação internacional?
  - impraticável
  - opções?
    - Convenção de Budapeste – 32b
    - necessidade de ir mais longe

ir mais longe?

Convenção de Budapeste – 32b

- consentimento para aceder:
  - informação pode ser usada

Lei Portuguesa (Lei nº 109/2009, de 15 de Setembro)

- *consentimento para aceder:*
  - *informação pode ser usada*
- *sem consentimento para aceder:*
  - *Artigo 15, 1 e 5*
  - *o Ministério Público pode ordenar a extensão da pesquisa*

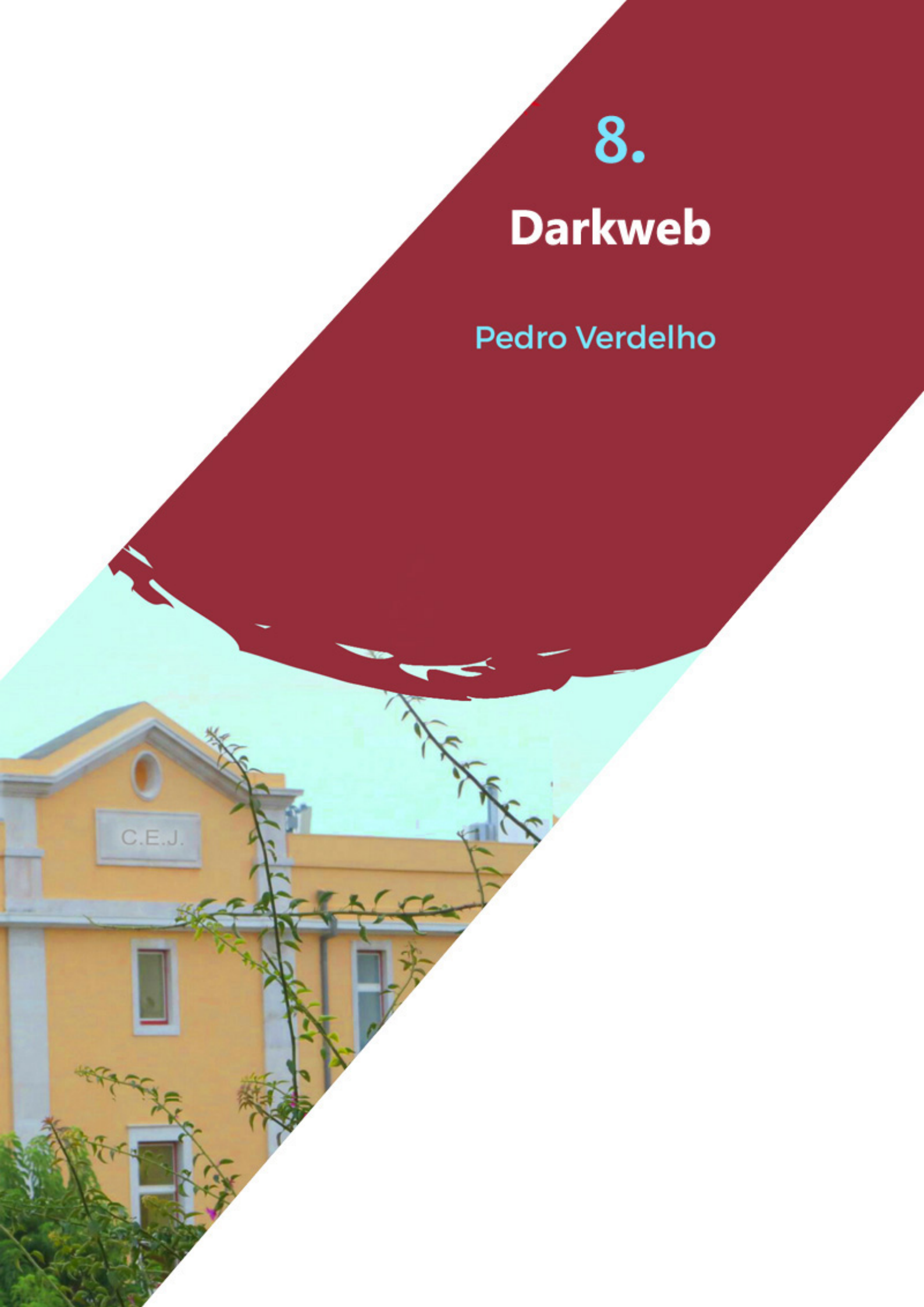
Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/gw3f7ymjz/flash.html?locale=pt

8.

Darkweb

Pedro Verdelho



CENTRO
DE ESTUDOS
JUDICIÁRIOS

8. DARKWEB

Pedro Verdelho*

Apresentação *Power Point*
Vídeo

Apresentação *Power Point*

* Procurador da República, Coordenador do Gabinete Cibercrime da PGR.

MINISTÉRIO PÚBLICO
PORTUGAL
gabinete CIBERCRIME

FONTE:
http://image.slidesharecdn.com/thedarkweb-140913103352-phpapp01/95/the-dark-web-3-638.jpg?cb=1410604462

DARKWEB

- Pequenas redes *peer to peer*
- Que constituem grandes redes (TOR, Freenet, I2P)

TOR

- conjunto de servidores (geridos por voluntários)
- permitem comunicar em privacidade e segurança
  (como se fossem túneis, através da Internet)

DARKWEB

Permite

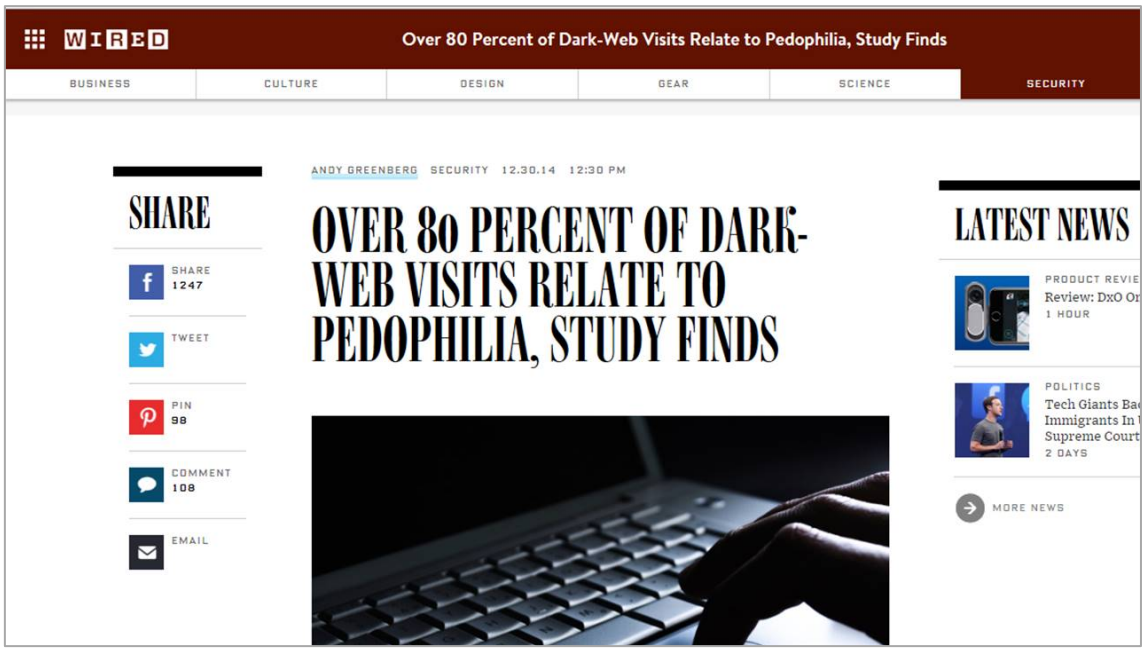
- manter websites em local escondido
- aceder a websites sem ser detetado
- comunicar com outrém anonimamente

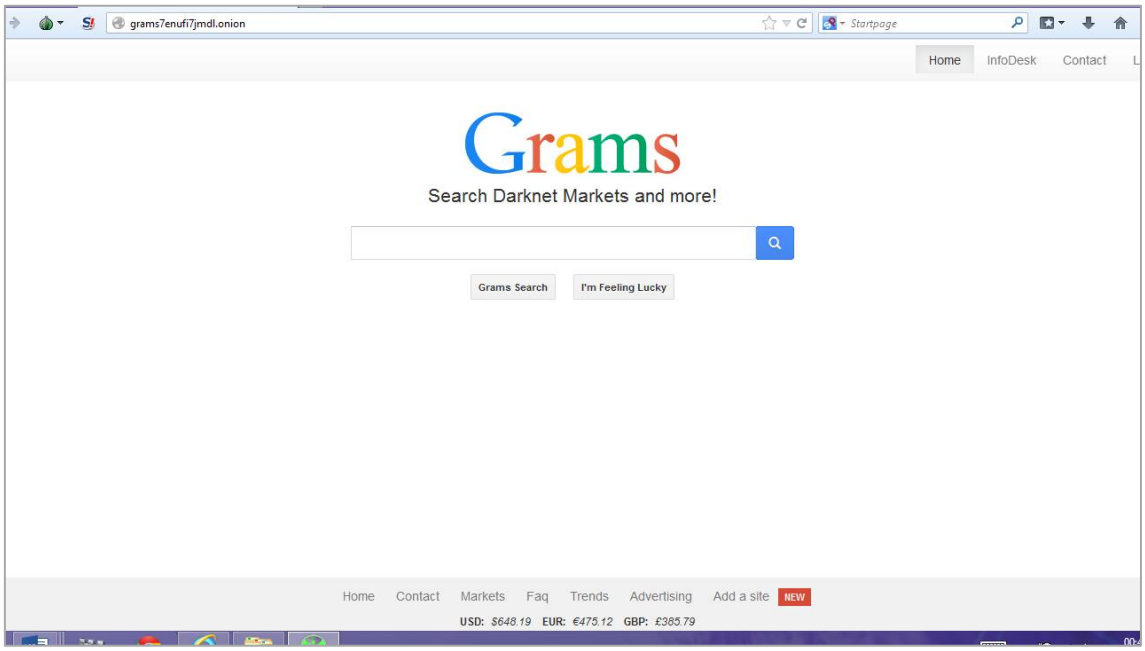
  - **jornalistas** (para comunicar com informadores ou dissidentes politicos)
  - Organizações de Direitos Humanos
  - **empresas** (para preservar os seus segredos comerciais)
  - **polícias** (em ações encobertas, para não sejam detetadas)

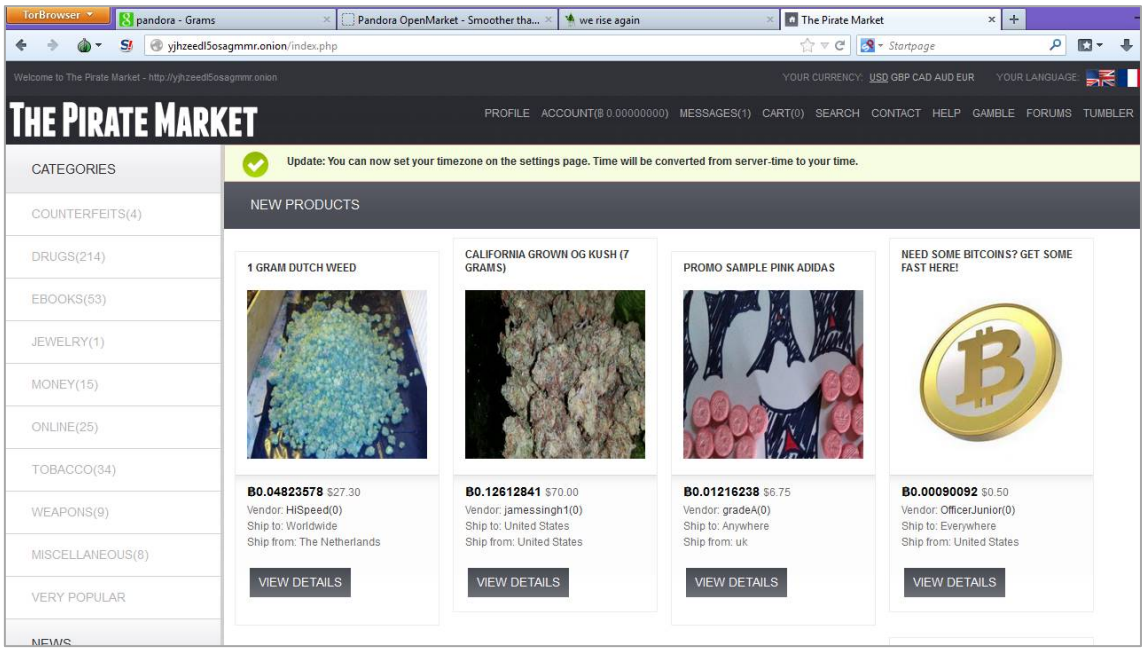
DARKWEB

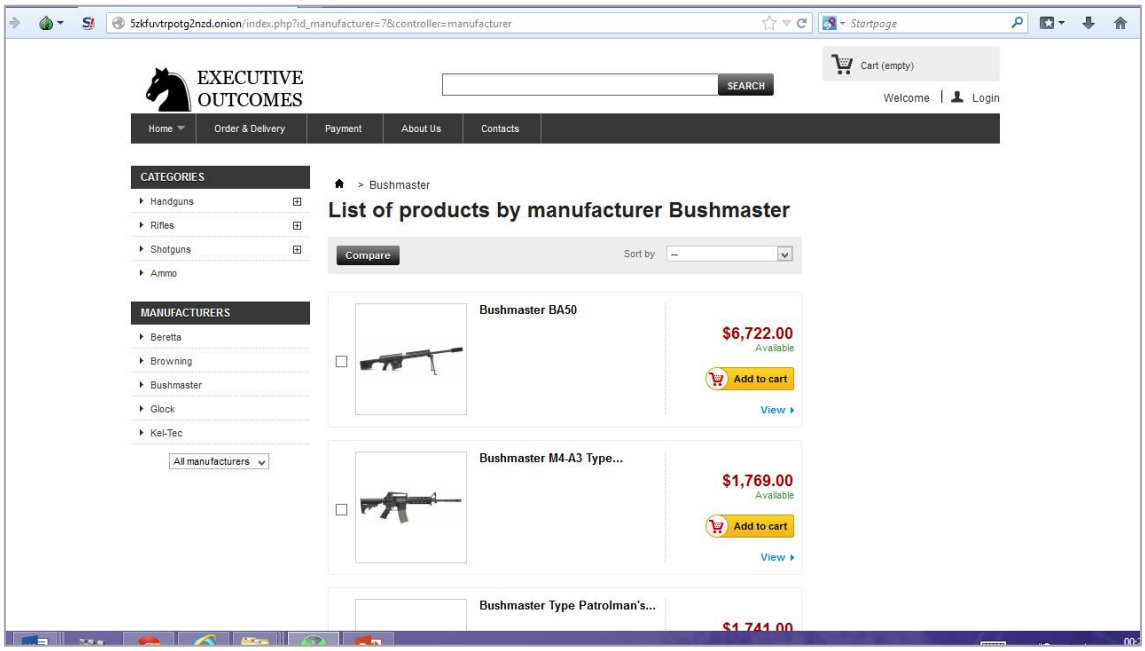
Para além disso….

Os mercados ilegais (droga, armas, pornografia infantil…)
O apoio ao terrorismo
Etc…


WIRED
Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds
BUSINESS
CULTURE
DESIGN
GEAR
SCIENCE
SECURITY
SHARE
SHARE 1247
TWEET
PIN 98
COMMENT 108
EMAIL
ANDY GREENBERG SECURITY 12.30.14 12:30 PM
OVER 80 PERCENT OF DARK-WEB VISITS RELATE TO PEDOPHILIA, STUDY FINDS
LATEST NEWS
PRODUCT REVIE
Review: DxO Or
1 HOUR
POLITICS
Tech Giants Ba
Immigrants In
Supreme Court
2 DAYS
MORE NEWS


grams7enufi7jmdl.onion
Startpage
Home
InfoDesk
Contact
Grams
Search Darknet Markets and more!
Grams Search
I'm Feeling Lucky
Home
Contact
Markets
Faq
Trends
Advertising
Add a site
NEW
USD: $648.19 EUR: €475.12 GBP: £385.79


THE PIRATE MARKET
PROFILE ACCOUNT(฿ 0.00000000) MESSAGES(1) CART(0) SEARCH CONTACT HELP GAMBLE FORUMS TUMBLER
CATEGORIES
COUNTERFEITS(4)
DRUGS(214)
EBOOKS(53)
JEWELRY(1)
MONEY(15)
ONLINE(25)
TOBACCO(34)
WEAPONS(9)
MISCELLANEOUS(8)
VERY POPULAR
Update: You can now set your timezone on the settings page. Time will be converted from server-time to your time.
NEW PRODUCTS
1 GRAM DUTCH WEED
B0.04823578 $27.30
Vendor: HiSpeed(0)
Ship to: Worldwide
Ship from: The Netherlands
VIEW DETAILS
CALIFORNIA GROWN OG KUSH (7 GRAMS)
B0.12612841 $70.00
Vendor: jamessingh1(0)
Ship to: United States
Ship from: United States
VIEW DETAILS
PROMO SAMPLE PINK ADIDAS
B0.01216238 $6.75
Vendor: gradeA(0)
Ship to: Anywhere
Ship from: uk
VIEW DETAILS
NEED SOME BITCOINS? GET SOME FAST HERE!
B0.00090092 $0.50
Vendor: OfficerJunior(0)
Ship to: Everywhere
Ship from: United States
VIEW DETAILS


EXECUTIVE OUTCOMES
SEARCH
Cart (empty)
Welcome | Login
Home
Order & Delivery
Payment
About Us
Contacts
CATEGORIES
Handguns
Rifles
Shotguns
Ammo
MANUFACTURERS
Beretta
Browning
Bushmaster
Glock
Kel-Tec
All manufacturers
> Bushmaster
List of products by manufacturer Bushmaster
Compare
Sort by
Bushmaster BA50
$6,722.00
Available
Add to cart
View
Bushmaster M4-A3 Type...
$1,769.00
Available
Add to cart
View
Bushmaster Type Patrolman's...

localização desconhecida

anonimato

E isto importa?

- prova espalhada a nível global
  - localmente, em dispostivos
  - provavelmente também algures no mundo
  - necessidade de a obter fora das nossas fronteiras

- prova "em lado nenhum"

Questões difíceis:

local da prática do crime
qual a **lei penal** substantiva **aplicável**
Portugal é competente?
Código Penal aplica-se?

a **jurisdição nacional** é um **limite à investigação**
investigações transfronteiriças?
investigações na "cloud"?

Questões difíceis:

local da prática do crime
qual a **lei penal** substantiva **aplicável**
Portugal é competente?
Código Penal aplica-se?

a **jurisdição nacional** é um **limite à investigação**
investigações transfronteiriças?
investigações na "cloud"?

convenção de Budapeste sobre cibercrime

Artigo 32º
Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

(…)

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, **se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados**, através deste sistema informático.

convenção de Budapeste sobre cibercrime

- aberta à assinatura a 21 de Novembro de 2001
- em vigor desde 2004 – para Portugal, desde 2009
- o primeiro (e único em vigor) tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados
- vocação universal
- cerca de 70 países

convenção de Budapeste sobre cibercrime

Artigo 32º
Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

(…)

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, **se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados**, através deste sistema informático.

- localização dos dados?
- quem pode autorizar o acesso aos dados?

MINISTÉRIO PÚBLICO PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

Lei nº 109/2009 - Lei do Cibercrime

Artigo 15º
Pesquisa de dados informáticos

(...)

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os **dados procurados se encontram noutro sistema informático**, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, **a pesquisa pode ser estendida** mediante autorização ou ordem da autoridade competente, nos termos dos nºs 1 e 2.

MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

Rua do Vale de Pereiro nº 2, 2º 1269-113 LISBOA
cibercrime@pgr.pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

9.

O Phishing: apresentação e análise de caso típico

Fernanda Pêgo
e
Carlos Nunes

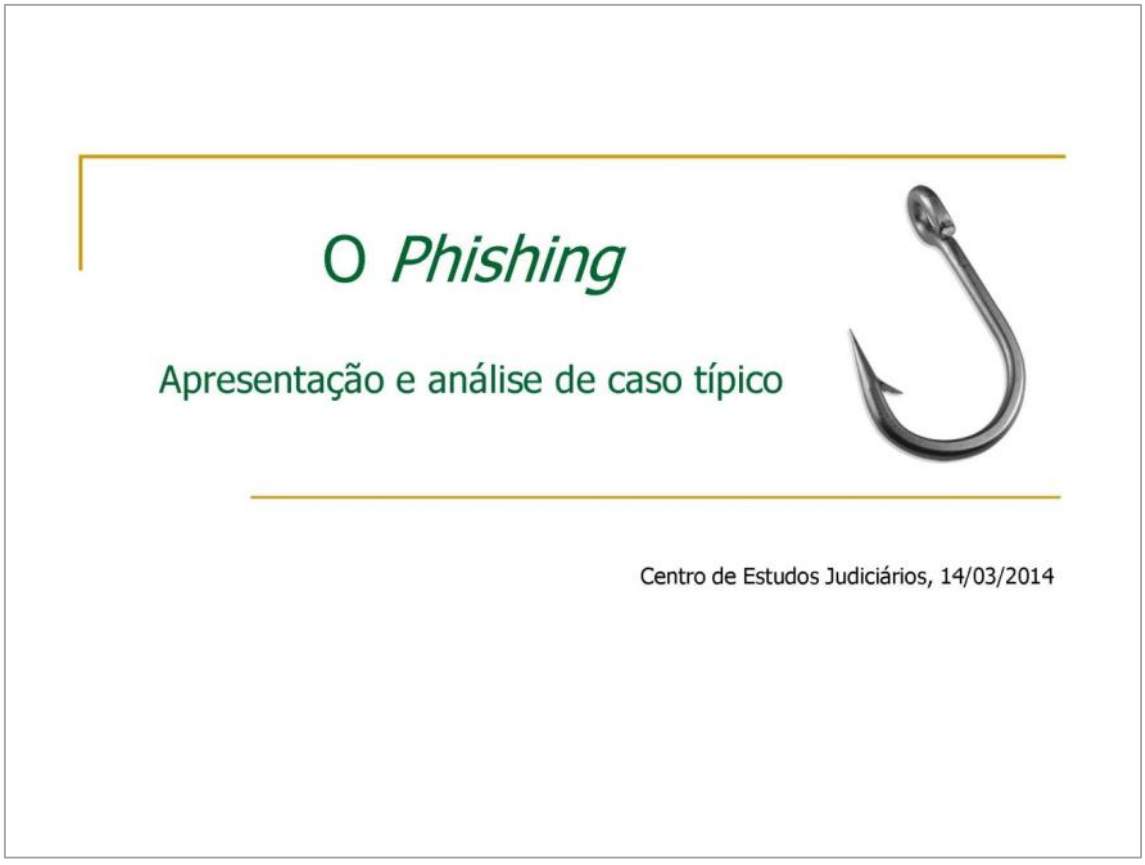
CENTRO
DE ESTUDOS
JUDICIÁRIOS

9. O PHISHING: APRESENTAÇÃO E ANÁLISE DE CASO TÍPICO[1]

Fernanda Pêgo*
Carlos Nunes**

Apresentação *Power Point*
Vídeos

Apresentação *Power Point*



[1] O texto corresponde às notas que serviram de apoio à intervenção do autor na ação de formação "Cibercriminalidade", no CEJ, no dia 14 de março de 2014.

* Procuradora da República, Coordenadora no Departamento de Investigação e Ação Penal de Lisboa.
** Inspetor da Polícia Judiciária.

Agenda

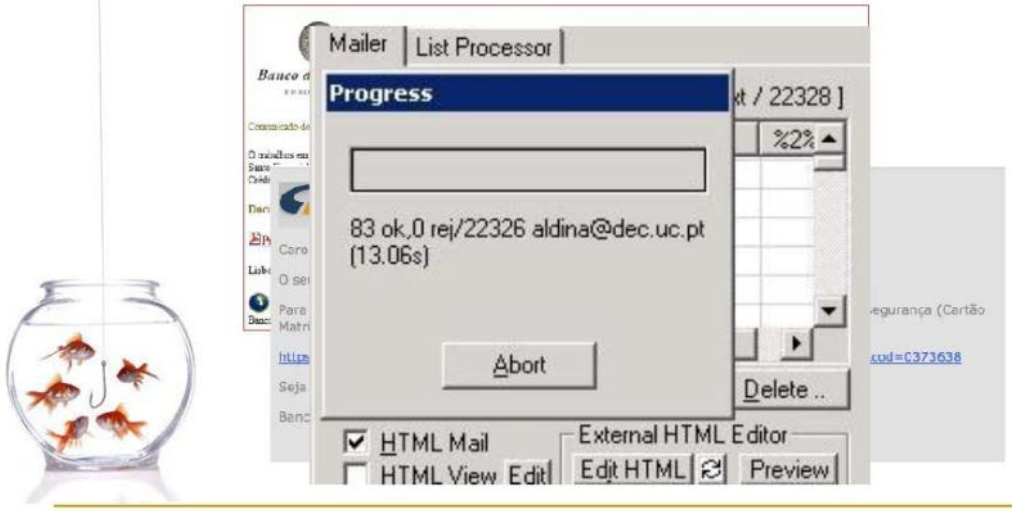
i. Introdução ao *modus operandi*
ii. Vectores de actuação
iii. Abordagem proactiva
iv. O caso concreto

Introdução ao *modus operandi*

i. Desenvolvimento de ferramentas de captura de dados, e respectiva disseminação;
ii. Angariação de conta de destino dos fundos a transferir, para posterior distribuição dos proventos ilícitos;
iii. Acesso à conta bancária do ofendido e realização da movimentação ilícita;
iv. Distribuição dos valores obtidos.

i - Desenvolvimento de ferramentas de captura de dados e respectiva disseminação

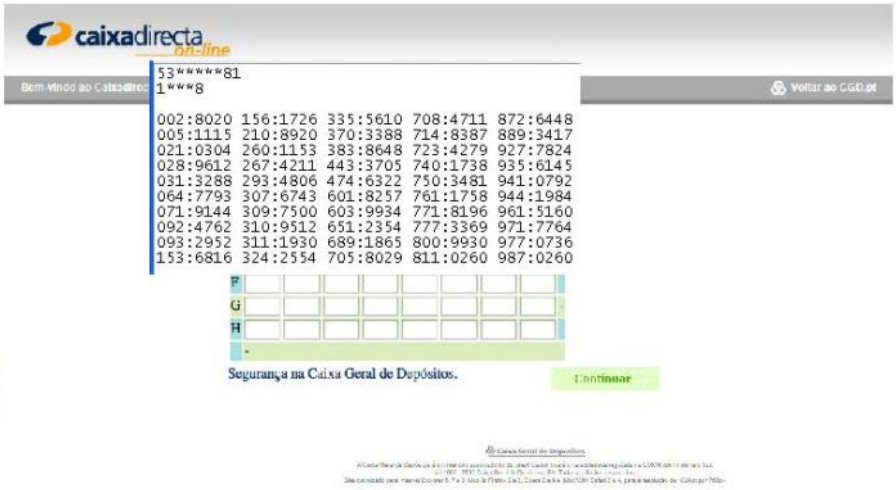
- Spam – Correio eletrónico não solicitado



i - Desenvolvimento de ferramentas de captura de dados e respectiva disseminação

i - Desenvolvimento de ferramentas de captura de dados e respectiva disseminação

- Contribuição voluntária da vítima



ii - Angariação de conta de destino dos fundos a transferir

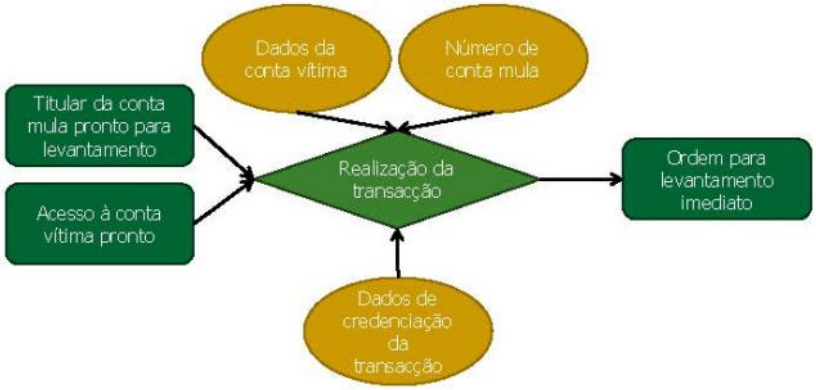
- Necessidade de garantir a fidelidade do titular da conta de destino (conta mula)

€

i. Job scam
ii. Meio social

iii - Acesso à conta bancária do ofendido e realização da movimentação ilícita

- Necessidade de articulação dos diferentes intervenientes:



iv - Distribuição dos valores obtidos

i. Job scam:
   i. Levantamento em agência bancária
   ii. Remessa do valor para o estrangeiro via casas de câmbios
   iii. Remuneração da estrutura deduzida de "comissão"

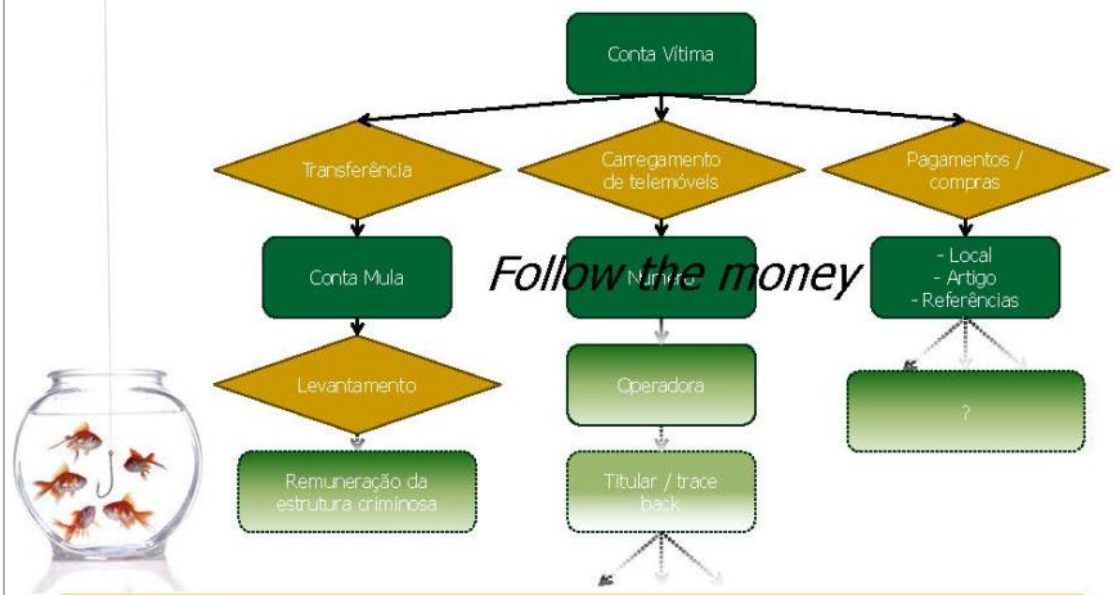
ii. Meio social:
   i. Compra de divisas / Casinos / Outras transacções de compra por cartão bancário
   ii. Remuneração da estrutura

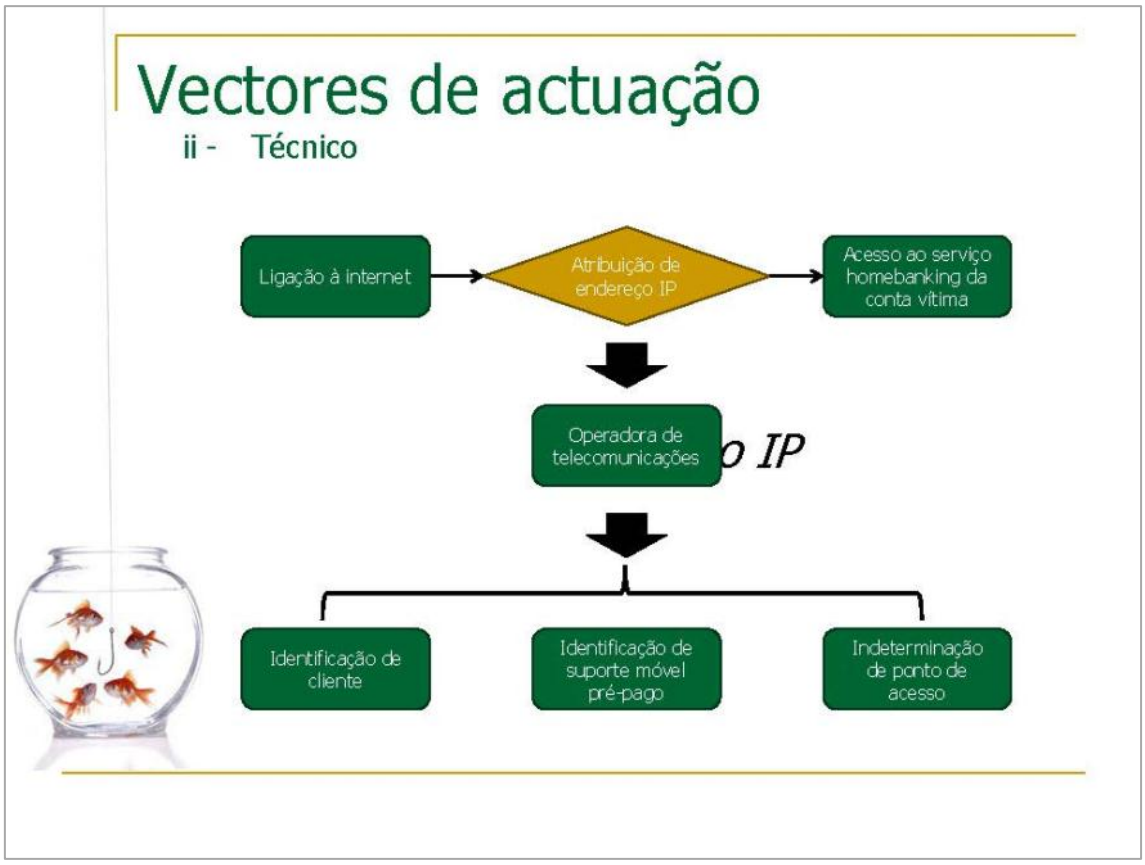
Vectores de actuação

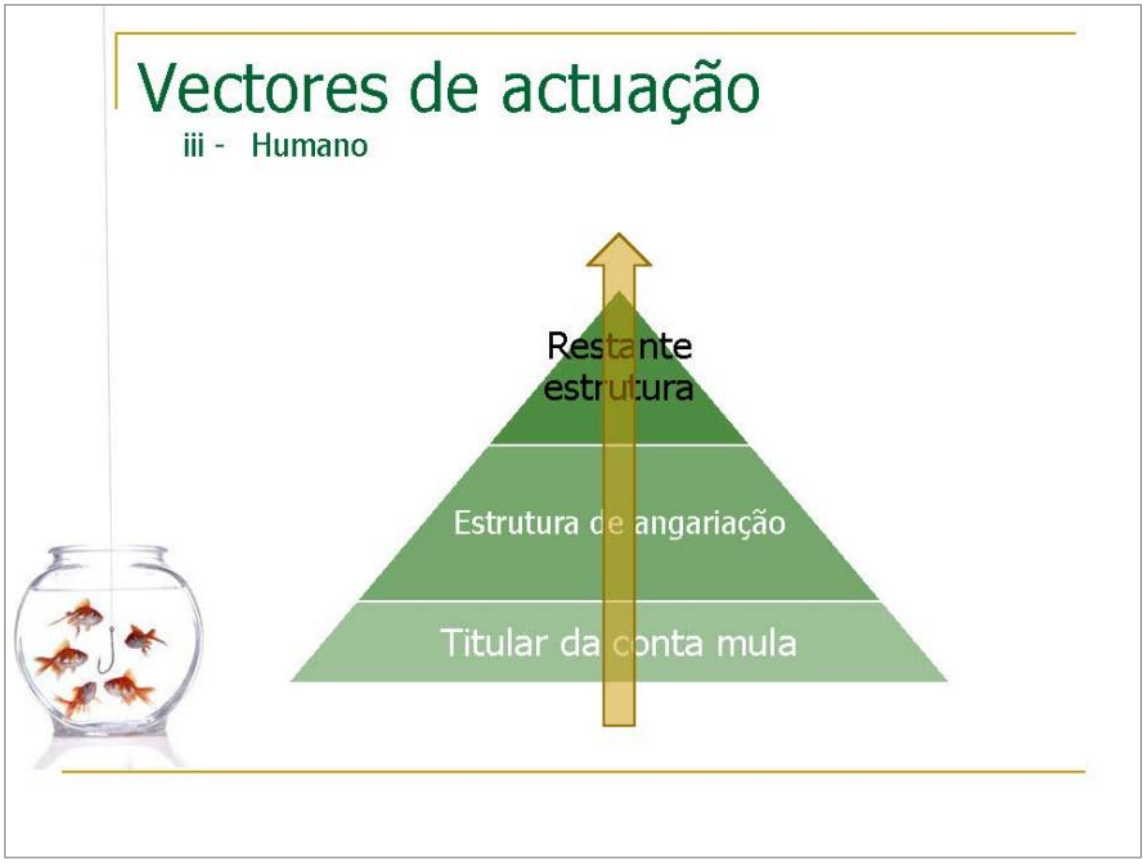
- Financeiro
- Técnico
- Humano

Vectores de actuação

i - Financeiro




Vectores de actuação
ii - Técnico
Ligação à internet
Atribuição de endereço IP
Acesso ao serviço homebanking da conta vítima
Operadora de telecomunicações
Identificação de cliente
Identificação de suporte móvel pré-pago
Indeterminação de ponto de acesso


Vectores de actuação
iii - Humano
Restante estrutura
Estrutura de angariação
Titular da conta mula

Abordagem proactiva

Constrangimentos à actuação célere

i. **Tempo de reacção:**
   i. Apresentação da denúncia
   ii. Remessa para o OPC competente
ii. **Constrangimentos legais:**
   i. Prazos de preservação CCTV
   ii. Sigilos bancário e nas telecomunicações

Abordagem proactiva

Diligências passíveis de execução imediata

i. Dados bancários
   i. **Conta do ofendido**
      i. Extracto de movimentos
      ii. Detalhe de transacção
      iii. Identificação endereço IP, grupo data hora e fuso horário num período de 15 dias antes da transacção, inclusive e com indicação desta
      iv. Identificação de conta destino
   ii. **Conta destino (imediato caso na mesma instituição)**
      i. Indicação da data de abertura
      ii. Cópia de ficha de identificação dos titulares e da ficha de assinaturas
      iii. Extracto de conta desde 15 dias antes dos factos e até 5 dias depois destes;
      iv. Extracto de movimentos de cartão bancário, incluindo movimentos de consulta, desde 1 dias antes dos factos e até 2 dias depois destes;
      v. Preservação CCTV e envio de documentação de suporte caso o levantamento tenha ocorrido perante qualquer balcão do banco;
      vi. Sendo identificado outro local de levantamento passível de recolha de imagens de videovigilância, seja esta informação prestada de imediato;
      vii. Informação sobre eventuais transferências realizadas para a conta de destino nos mesmos moldes da identificada

O caso prático - Sete Mares

i. A investigação em números
ii. O começo
iii. O desenho da estrutura nos diferentes vectores
iv. Os factos nos diferentes momentos
v. O crime em marcha

O caso prático - Sete Mares

Números

i. Período de investigação:
  i. Ago '12 – Denúncia inicial
  ii. Fev '13 – Cessação da actividade ilícita
  iii. Fev '14 – Conclusão da investigação
ii. Intercepções telefónicas:
  i. 50 alvos
  ii. > 250.000 sessões
iii. 16 buscas a residências e empresas
iv. 110 vítimas
v. 80 arguidos
vi. Prejuízo:
  i. Efectivo > € 240.000,00
  ii. Tentado > € 275.000,00

O caso prático - Sete Mares

Acção / Reacção

- Combinação *username/password*
- Senha de transacção
- Cartão matriz

→ Engenharia social / captura de dados

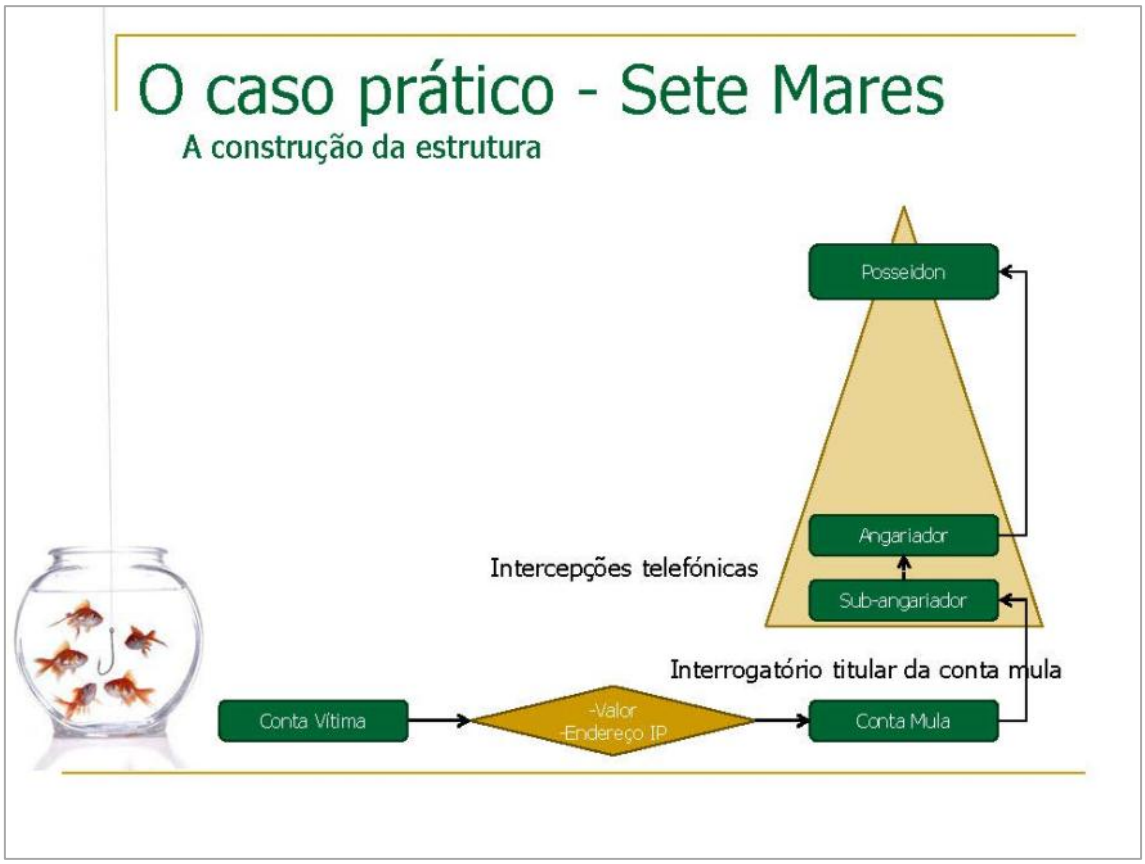
- Código sms → Compromisso da operadora de telecomunicações
- *Token device* → *man in the middle*

O caso prático - Sete Mares

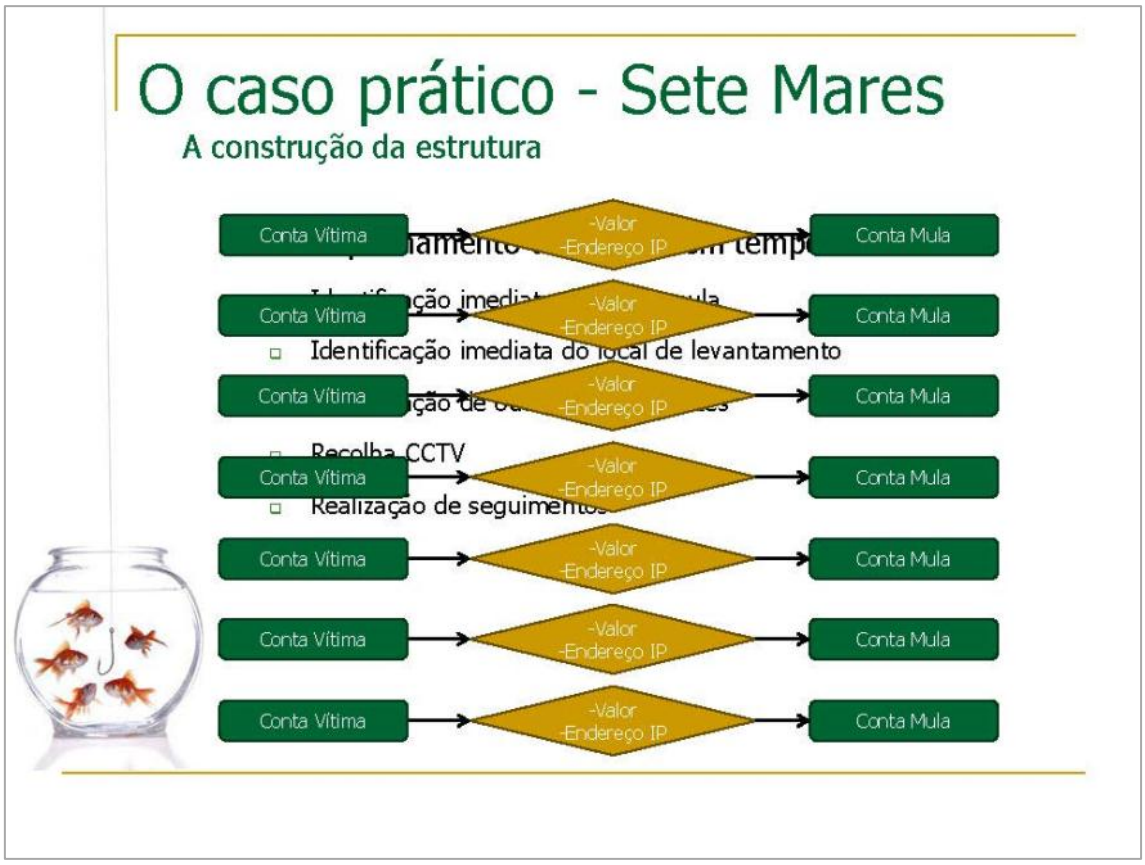
O começo

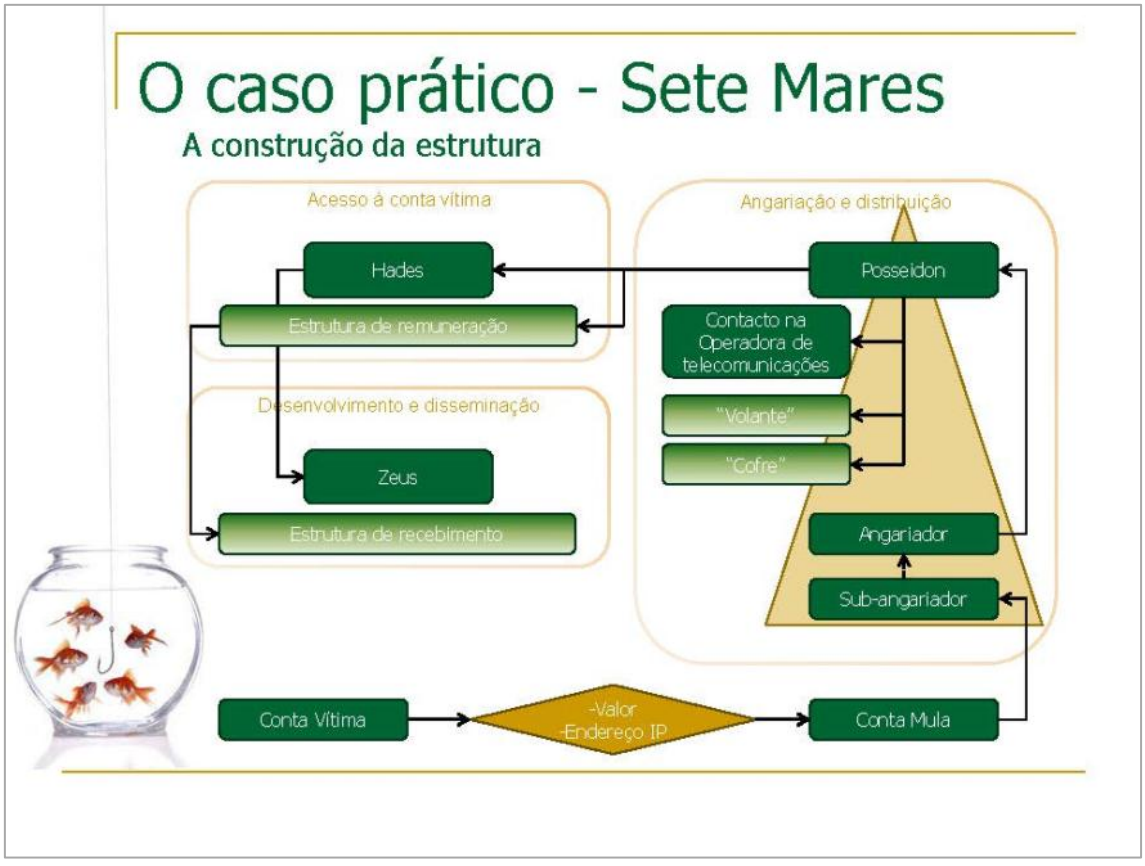
Interrogatório: 1 mês

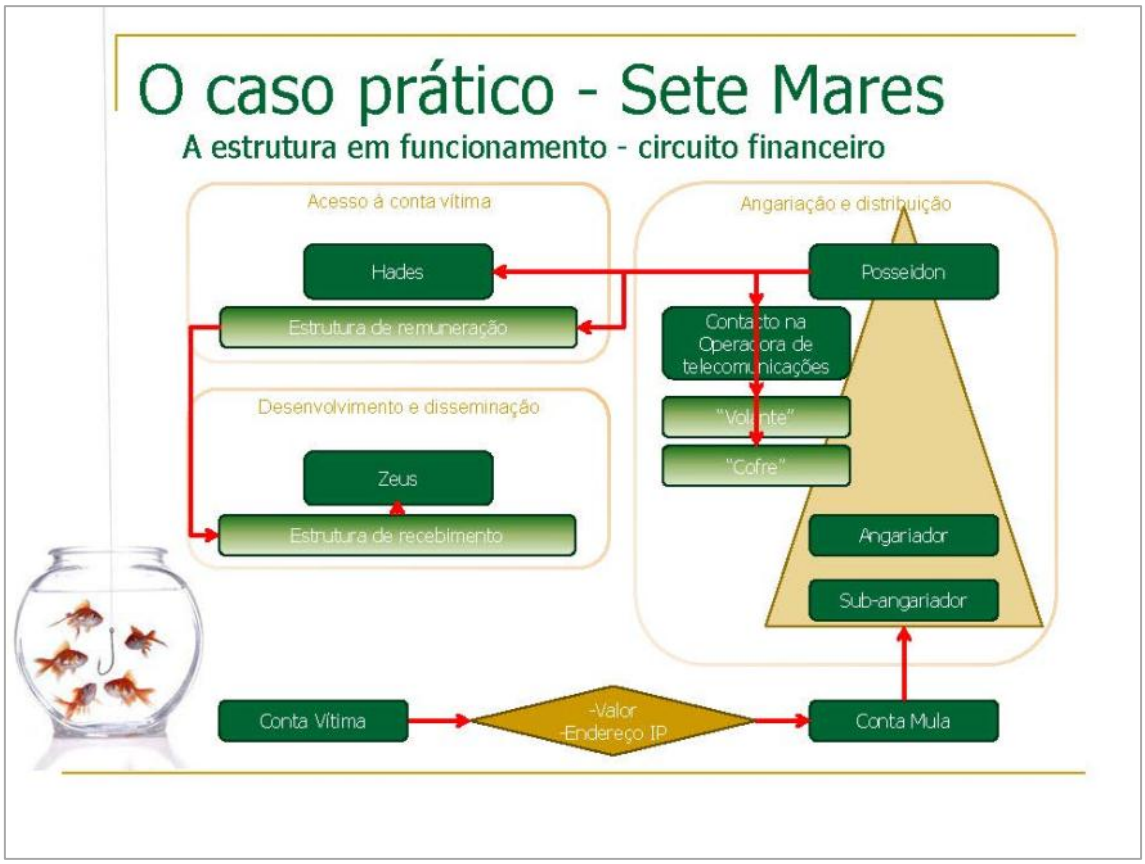
Conta Vítima → -20.000,00 Endereço IP → Conta Mula

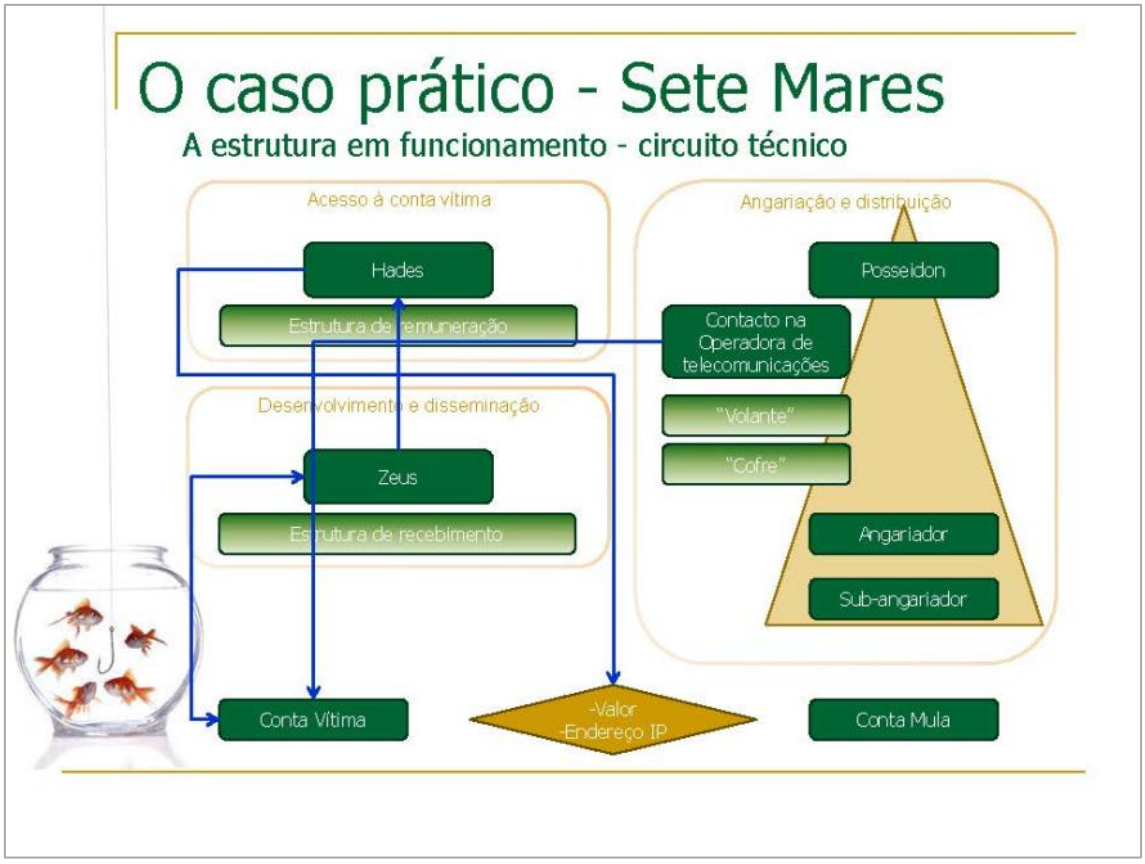

O caso prático - Sete Mares
A construção da estrutura
Posseidon
Angariador
Sub-angariador
Intercepções telefónicas
Interrogatório titular da conta mula
Conta Vítima
-Valor
-Endereço IP
Conta Mula

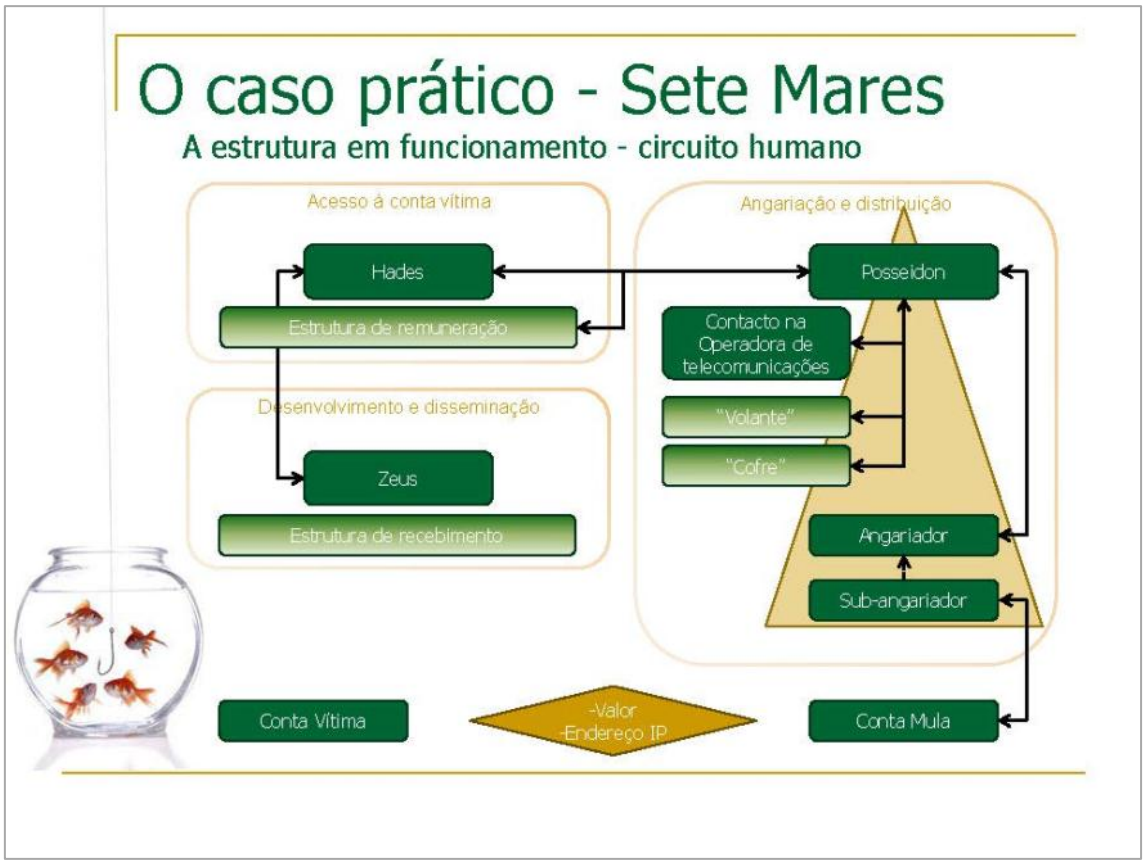

O caso prático - Sete Mares
A construção da estrutura
Conta Vítima
-Valor
-Endereço IP
Conta Mula
Intercepções telefónicas

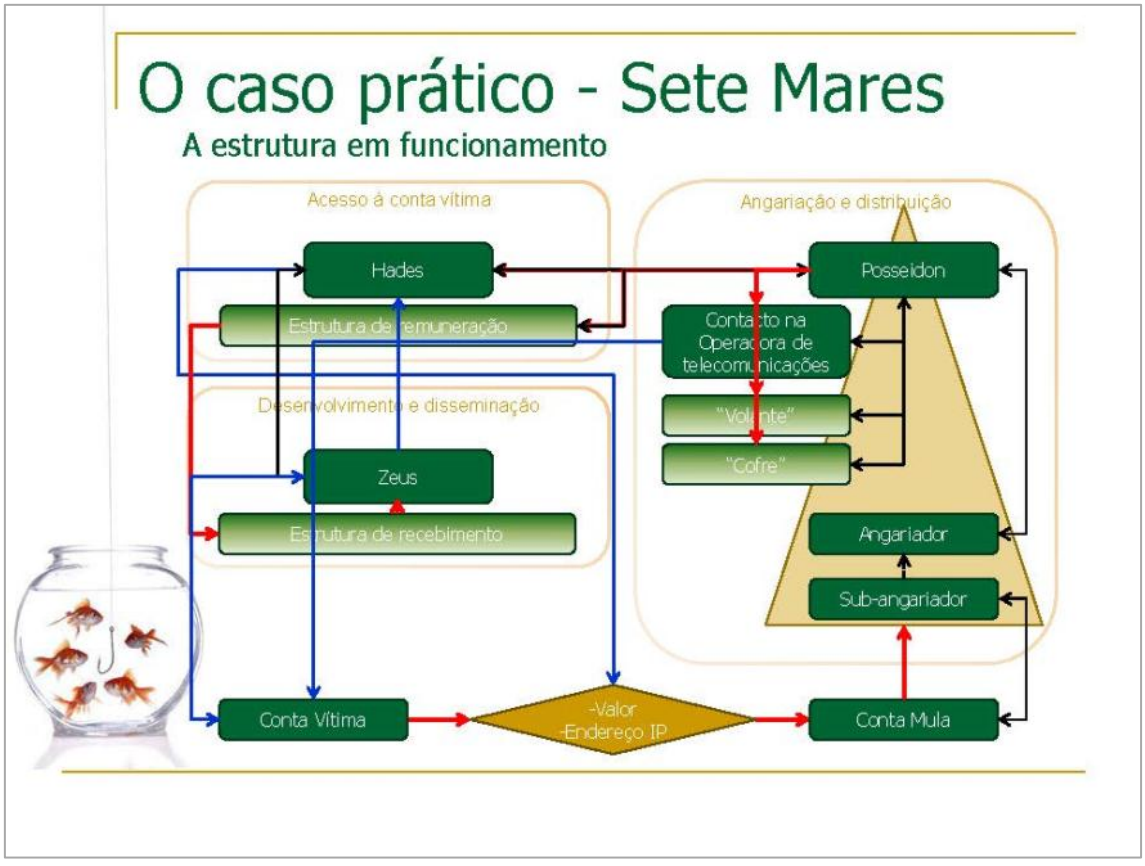

O caso prático - Sete Mares
A construção da estrutura
Conta Vítima
-Valor
-Endereço IP
Conta Mula
Identificação imediata do local de levantamento
Recolha CCTV
Realização de seguimentos


O caso prático - Sete Mares
A construção da estrutura
Acesso à conta vítima
Hades
Estrutura de remuneração
Desenvolvimento e disseminação
Zeus
Estrutura de recebimento
Angariação e distribuição
Posseidon
Contacto na Operadora de telecomunicações
"Volante"
"Cofre"
Angariador
Sub-angariador
Conta Vítima
-Valor
-Endereço IP
Conta Mula


O caso prático - Sete Mares
A estrutura em funcionamento - circuito financeiro
Acesso à conta vítima
Hades
Estrutura de remuneração
Desenvolvimento e disseminação
Zeus
Estrutura de recebimento
Angariação e distribuição
Posseidon
Contacto na Operadora de telecomunicações
"Volante"
"Cofre"
Angariador
Sub-angariador
Conta Vítima
-Valor
-Endereço IP
Conta Mula

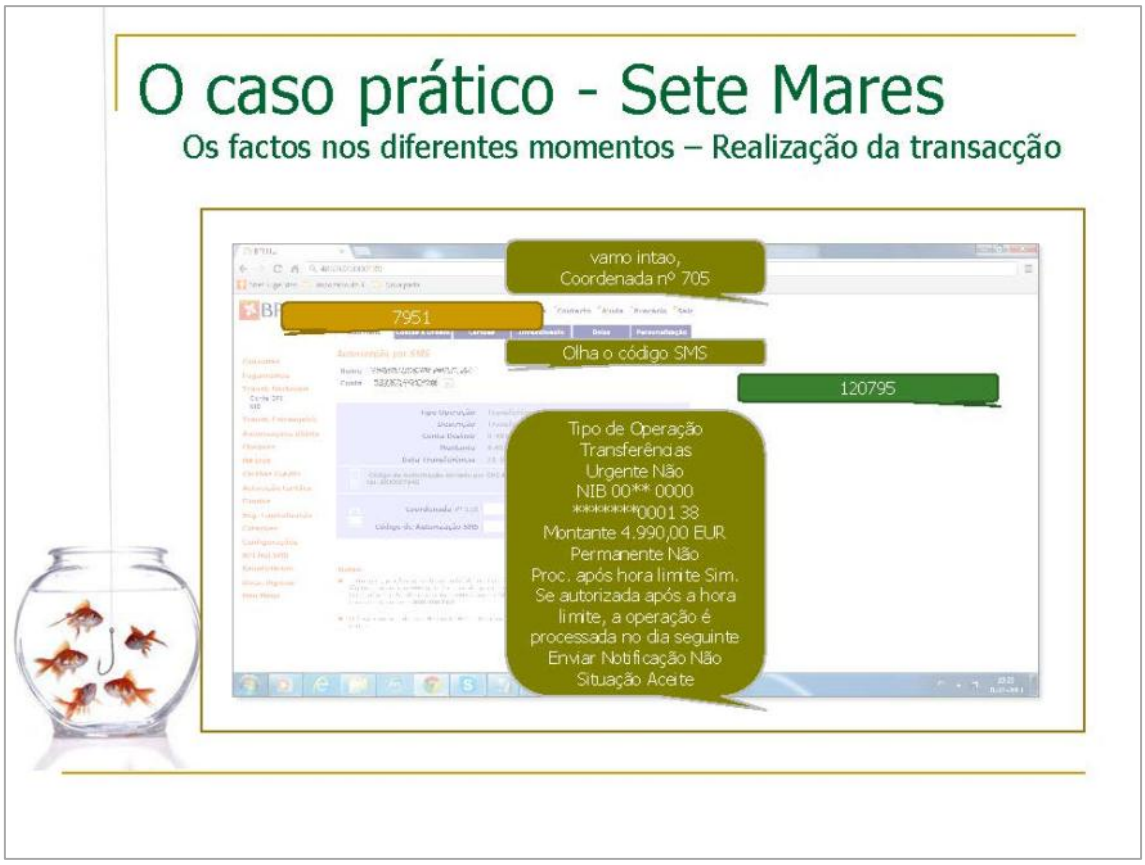

O caso prático - Sete Mares
A estrutura em funcionamento - circuito técnico
Acesso à conta vítima
Hades
Estrutura de remuneração
Desenvolvimento e disseminação
Zeus
Estrutura de recebimento
Angariação e distribuição
Posseidon
Contacto na Operadora de telecomunicações
"Volante"
"Cofre"
Angariador
Sub-angariador
Conta Vítima
-Valor
-Endereço IP
Conta Mula

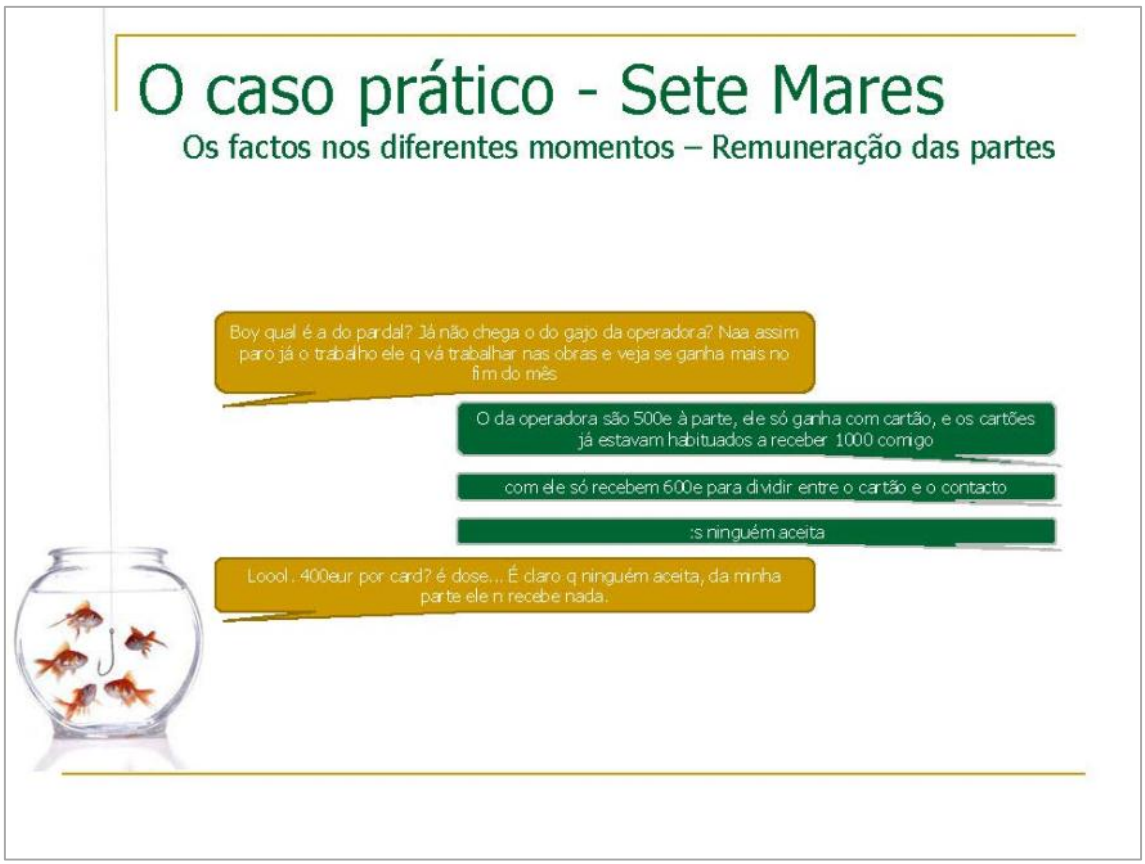

O caso prático - Sete Mares
A estrutura em funcionamento - circuito humano
Acesso à conta vítima
Angariação e distribuição
Hades
Posseidon
Estrutura de remuneração
Contacto na Operadora de telecomunicações
Desenvolvimento e disseminação
"Volante"
"Cofre"
Zeus
Angariador
Estrutura de recebimento
Sub-angariador
Conta Vítima
-Valor
-Endereço IP
Conta Mula


O caso prático - Sete Mares
A estrutura em funcionamento
Acesso à conta vítima
Angariação e distribuição
Hades
Posseidon
Estrutura de remuneração
Contacto na Operadora de telecomunicações
Desenvolvimento e disseminação
"Volante"
"Cofre"
Zeus
Angariador
Estrutura de recebimento
Sub-angariador
Conta Vítima
-Valor
-Endereço IP
Conta Mula


O caso prático - Sete Mares
Os factos nos diferentes momentos - Angariação
puto caderneta dá?
caderneta nao dá boy tens q ter multibanco pq nas casa de cambio tem q ser com MB
e ele vai la com o multibanco e levanta na boa?
no multibanco nao consegues levantar 5000mil, tem q ir a casa de cambio com o cartao e dizer q quer 5mil eur em dolar ou libra
e de certeza que da?
Ya, tem q ser rapido a sacar, no maximo 15m
ya, em que sitios se pode levantar?
casa de cambio
e isso depois não dá espiga
não boy. depois ele só tem é que dizer no banco que perdeu o cartão com o código, ou que fez um favor a alguém e isso depois não dá nada


O caso prático - Sete Mares
Os factos nos diferentes momentos - Angariação
Iá boy!
Iá, olha...
Hã?
Tá aí por tudo por cada.
Iá, eu vi, eu vi.
E faz uma coisa, amanhã, tipo, organiza, tipo, vai ao BPI abres conta às pessoas com vinte e cinco euros e dão-te logo o cartão na mão.
O quê? O quê?
Eu disse, amanhã vais com as pessoas ao Banco, abres conta no BPI, eles dão-te logo o cartão provisório. Ficas tu com o cartão e depois fazes.


O caso prático - Sete Mares
Os factos nos diferentes momentos – Realização da transacção
vamo intao, Coordenada nº 705
7951
Olha o código SMS
120795
Tipo de Operação Transferências
Urgente Não
NIB 00** 0000 ********0001 38
Montante 4.990,00 EUR
Permanente Não
Proc. após hora limite Sim. Se autorizada após a hora limite, a operação é processada no dia seguinte
Enviar Notificação Não
Situação Aceite


O caso prático - Sete Mares
Os factos nos diferentes momentos – Remuneração das partes
Boy qual é a do pardal? Já não chega o do gajo da operadora? Naa assim paro já o trabalho ele q vá trabalhar nas obras e veja se ganha mais no fim do mês
O da operadora são 500e à parte, ele só ganha com cartão, e os cartões já estavam habituados a receber 1000 comigo
com ele só recebem 600e para dividir entre o cartão e o contacto
:s ninguém aceita
Loool. 400eur por card? é dose... É claro q ninguém aceita, da minha parte ele n recebe nada.

O caso prático - Sete Mares

Os factos nos diferentes momentos – Remuneração das partes

O caso prático - Sete Mares

Os factos nos diferentes momentos - Impunidade

Iá, ele disse-me isso.... Ele disse-me "iá, em princípio não vai haver nenhum problema. Agora as pessoas..." Eu disse "Que banco". Não vai haver nenhum problemas mas que as pessoas que lhes foi retirado o dinheiro, tás a ver, é que podem fazer alguma coisa, tipo um advogado ou assim e querer saber mais a situação. Porque em princípio, com o banco mesmo não vai haver mesmo problema. Eu só vou ficar sem a conta até, tipo, até eles saberem o que é que realmente aconteceu.

Mas também as pessoas que ficarem sem o dinheiro... e se quiserem avançar com alguma coisa para a frente eles é que ficam a perder porque supostamente vão ter que pagar advogados, abrir processos, não sei quê não sei que mais. Vamos a ver nunca vai compensar nada daqueles coiso... não vai compensar nada aquilo que eles estão a gastar. E depois o banco também nunca lhes vai informações suficientes para eles continuarem a avançar com o caso. É tanto como montes de casos que já fizeram... que me têm vindo a dizer, tipo no *facebook* ou quando me encontram dizem sempre "ah o meu caso foi arquivado por falta de prova e não sei quê não sei que mais porque o banco não permite". Iá, eles nunca vão a lado nenhum, e se eles quiserem abrir um inquérito só têm a perder.

O caso prático - Sete Mares

Os factos nos diferentes momentos – O crime em marcha

Sex, 01/01/1999 16:50

mano veja 1º uma conta para carregar o tlm, fiquei sem saldo

Contrato: Pinh160594
Senha: 7***3

essa tem saldo, vou carregar. Coordenada nº 57?

2219

feito :D
pra ver essas particulares ou vamos já nas empresas ?

vamos nas empresas

O *Phishing*

Apresentação e análise de caso típico

Fernanda Pêgo
Procuradora da República Coordenadora
Departamento de Investigação e Ação Penal de Lisboa

Carlos Nunes
Inspetor
Policia Judiciária

Vídeos da apresentação

1. https://elearning.cej.mj.pt/mod/url/view.php?id=7032
2. https://elearning.cej.mj.pt/mod/url/view.php?id=7034
3. https://elearning.cej.mj.pt/mod/url/view.php?id=7036
4. https://elearning.cej.mj.pt/mod/url/view.php?id=7033
5. https://elearning.cej.mj.pt/mod/url/view.php?id=7035

Título:
Cibercriminalidade e Prova Digital

Ano de Publicação: 2018

ISBN: 978-989-8908-17-9

Série: Formação Contínua

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt