



FACULDADE DE DIREITO
Universidade de Lisboa

Ficha de unidade curricular

Curso de Mestrado em Ciências Jurídico-Forenses
(2.º Ciclo)
2.º Semestre

Unidade curricular

Direito Penal V

Docente responsável e respetiva carga letiva na unidade curricular (preencher o nome completo)

Paulo Manuel Mello de Sousa Mendes – 2 horas

Outros docentes e respetivas cargas letivas na unidade curricular

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes)

A Lei n.º 109/09 (Lei do Cibercrime) transpõe para a ordem jurídica interna a Decisão-Quadro relativa a ataques contra sistemas de informação e adaptou o Direito interno à Convenção sobre Cibercrime. São objetivos do presente curso fornecer uma visão pormenorizada e crítica da Lei do Cibercrime, quer no plano substantivo (crimes informáticos), quer no plano adjetivo (normas processuais e probatórias).

Conteúdos programáticos

Título I – APRESENTAÇÃO DA DISCIPLINA

O programa

Os instrumentos internacionais e supranacionais

A jurisprudência do TEDH

A jurisprudência do TJUE

Os direitos estrangeiros e o direito comparado

A Lei do Cibercrime

Título II – O CIBERCRIME

Os crimes informáticos da Lei do Cibercrime

Os crimes informáticos do Código Penal

Os crimes cometidos por meio de um sistema informático

Os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico

Título III – OS CRIMES INFORMÁTICOS EM ESPECIAL

A falsidade informática (art. 3.º LCib) vs. a falsificação de documento (art. 256.º CP)

O dano relativo a programas e outros dados informáticos (art. 4.º LCib) vs. o crime de dano (art. 212.º CP)

A sabotagem informática (art. 5.º LCib) vs. o crime de dano em instalações e perturbação de serviços (art. 277.º/1 d) CP) e o crime de sabotagem (art. 329.º CP)

O acesso ilegítimo (art. 6.º LCib)

A interceção ilegítima (art. 7.º LCib)

A reprodução ilegítima de programa protegido (art. 8.º LCib)

A devassa por meio de informática (artigo 193.º CP)

A burla informática (artigo 221.º CP) vs. a burla clássica (art. 217.º CP)

Os problemas do concurso de normas e do concurso de infrações

A responsabilidade penal das pessoas coletivas e equiparadas (art. 9.º LCib)

A perda de bens (art. 10.º LCib) e a perda alargada



FACULDADE DE DIREITO
Universidade de Lisboa

Título IV – A PROVA DIGITAL

O conceito e as especificidades da prova digital
O quadro legal vigente entre o CPP, a Lei do Cibercrime e a Lei n.º 32/2008, de 17 de julho
A jurisprudência do TJUE em matéria de conservação de dados de tráfego
A preservação expedita de dados (art. 12.º LCib)
A revelação expedita de dados de tráfego (art. 13.º LCib)
A injunção para apresentação ou concessão do acesso a dados (art. 14.º LCib)
A pesquisa e apreensão de dados informáticos (arts. 15.º e 16.º LCib)
A apreensão de correio eletrónico e de registos de comunicações de natureza semelhante (art. 17.º LCib)
A interceção de comunicações (art. 18.º LCib)
As ações encobertas digitais (art. 19.º LCib)
A monitorização on-line e a falta de norma habilitante
A investigação criminal na Dark Web
A utilização de armadilhas digitais
A prova digital obtida por particulares e investigadores privados

TÍTULO V – A CADEIA DE CUSTÓDIA DIGITAL

A cadeia de custódia e a validade da prova
O valor da privacidade defronte da recolha de prova digital (art. 8.º CEDH)
A jurisprudência do TEDH
As Federal Guidelines for Searching and Seizing Computers
A jurisprudência norte-americana
A Plain View Doctrine e a Cyberplain View

TÍTULO V – A COOPERAÇÃO JUDICIÁRIA INTERNACIONAL

O acesso unilateral a dados armazenados em sistemas informáticos localizados no estrangeiro
O âmbito da cooperação judiciária internacional

TÍTULO VI - A INTELIGÊNCIA ARTIFICIAL APLICADA AO DIREITO

Os sistemas periciais de auxílio à decisão judicial
A representação e a formalização do conhecimento jurídico
Os Big Data e a investigação criminal
A mineração de dados relevantes para a questão de facto
Os sistemas de apoio à motivação da questão de direito
Os sistemas automáticos de decisão judicial e o problema do juiz-robô

TÍTULO VII – OS AGENTES INTELIGENTES E A RESPONSABILIDADE

As máquinas e a responsabilidade
Os veículos autónomos e o direito penal

Demonstração da coerência dos conteúdos programáticos com os objetivos da unidade curricular

O programa visa estruturar a matéria do Cibercrime e da Prova Digital de maneira a dar conta da sua complexidade teórica e do seu relevo para a prática jurídica.

O programa está feito de forma a dar uma visão global da matéria, mas não foi concebido no pressuposto de que todos, nem sequer a maioria dos assuntos tenham de ser escolhidos pela turma para a elaboração dos relatórios individuais. Pelo contrário, o programa está construído como se fosse uma lista de temas sugeridos aos alunos para os relatórios. Naturalmente, os temas escolhidos pelos alunos poderão variar de um para outro ano letivo. As escolhas até poderão extravasar dos temas do programa, desde que mantenham com estes alguma relação forte e sejam suficientemente fundamentadas. Ainda assim, o programa servirá de cenário para que as escolhas dos alunos não reflitam somente as



FACULDADE DE DIREITO
Universidade de Lisboa

suas pré-compreensões sobre os temas da cibercriminalidade e da prova digital, mas revelem já abertura às discussões contemporâneas nestas temáticas.

Tal abertura às discussões contemporâneas é, ademais, garantida pela lecionação obrigatória de alguns dos temas estruturantes do programa pelo professor regente ou por especialistas convidados.

A aplicação do programa promove a constituição de um acervo que é acessível – designadamente através da criação de uma pasta coletiva na Dropbox – a todos os alunos da turma desde a fase dos projetos de investigação até à versão consolidada dos mesmos, não obstante os relatórios serem trabalhos rigorosamente individuais. O facto de a turma conhecer os projetos de investigação em curso não prejudica a desejável competitividade científica entre todos os alunos, uma vez que os temas escolhidos são diferentes, a menos que possa haver interesse científico e prático no tratamento paralelo de distintas facetas dos mesmos temas. Por exemplo, um aluno poderá tratar dos aspetos tecnológicos da monitorização on-line (considerando que os alunos do Curso de Mestrado em Segurança de Informação e Direito no Ciberespaço não são licenciados em Direito) e outro poderá tratar da questão da falta de norma habilitante expressa para a monitorização on-line na ordem jurídica portuguesa (considerando que os alunos do Curso de Mestrado em Direito e Prática Jurídica dominam naturalmente a problemática jurídica em causa).

Terminada a avaliação dos alunos, o regente incentiva a publicação dos melhores relatórios em revistas que tenham revisão por pares (peer review), nacionais ou estrangeiras. A publicação contribuirá para o crescimento da massa crítica que já vai existindo entre nós no domínio da cibercriminalidade e da prova digital, além de que acalentará nos alunos uma atitude de maior ambição científica, num contexto em que os resultados dependem sobremaneira do empenhamento de cada qual.

Metodologias de ensino (avaliação incluída)

Nos termos do n.º 1 do artigo 30.º do Regulamento do Mestrado e do Doutoramento (a partir do ano letivo 2018-2019), a avaliação numa UC do Mestrado em Direito e Prática Jurídica compreende os seguintes elementos de aferição de conhecimentos:

- a) Uma prova escrita de avaliação final obrigatória;
- b) Outros elementos de avaliação, escrita e/ou oral, a determinar pelo docente responsável pela UC.

Nos termos do n.º 2 do artigo 30.º do Regulamento, a classificação final decorre da atribuição de 50 % da ponderação à prova escrita e os restantes 50 % são preenchidos pelos elementos de avaliação determinados pelo docente responsável pela UC, incluindo a assiduidade às aulas.

Na falta de definição, pelo docente responsável pela UC, da assiduidade mínima relevante, funciona como critério supletivo o da frequência, pelo estudante, de, pelo menos, metade das aulas. É sempre realizada a chamada no final de cada aula e são registadas as ausências, vulgo “faltas”. É permitida a entrada de alunos no decurso da aula, embora com expressa advertência de que tal deve ser evitado.

Na UC de Direito Penal V, é elemento da avaliação um relatório escrito final a apresentar por cada um dos estudantes inscritos, sendo tomadas em consideração para efeitos da avaliação também as pré-apresentações e apresentações orais dos relatórios ao longo do semestre letivo.

Também é avaliada a participação oral espontânea dos estudantes durante as aulas.

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

Os tempos letivos, num total de cerca de 15 aulas com a duração de 2 horas por sessão, seguem um modelo de aulas teórico-práticas. A aula introdutória inclui apresentação do programa e método de ensino. As seguintes seis aulas estão a cargo do regente e de especialistas convidados. Há ainda uma aula dedicada ao método de elaboração de relatórios científicos. Nesta aula, o regente faculta aos alunos um modelo de folha de apoio (handout) para a pré-apresentação e um formato-padrão (template) para o relatório, os quais ficam imediatamente disponíveis na DropBox criada especificamente para a turma na UC de Direito Penal V do Mestrado em Direito e Ciência Jurídica. A utilização de um formato-padrão facilita a harmonização formal de todos os trabalhos e faculta instruções mínimas sobre como fazer um trabalho de ciência jurídica.

As restantes aulas são preenchidas pela discussão dos trabalhos dos alunos.

Bibliografia principal

Título I - APRESENTAÇÃO DA DISCIPLINA

a) O programa

ASCENSÃO, José de Oliveira,



FACULDADE DE DIREITO
Universidade de Lisboa

(2001) *Estudos sobre Direito da Internet e da Sociedade da Informação*, Coimbra: Almedina.

CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo, e PAPA, Michele,

(2019) *Cybercrime*, Milano: UTET.

CASEY, Eoghan,

(2011) *Digital Evidence and Computer Crime – Forensic Science, Computers, and the Internet*, 3.^a ed., San Diego: Elsevier Science Publishing.

HILGENDORF, Eric, e VALERIUS, Brian,

(2012) *Computer- und Internetstrafrecht – Ein Grundriss*, 2.^a ed., Heidelberg/Dordrecht/London/New York: Springer.

KERR, Orin S.,

(2018) *Computer Crime Law*, 4.^a ed., St. Paul, MN: West Academic Publishing.

MARQUES, Garcia, e MARTINS, Lourenço,

(2006) *Direito da Informática*, 2.^a ed., Coimbra: Almedina (1.^a ed., 2001).

REED, Chris,

(2011) *Computer Law*, 7.^a ed., Oxford: Oxford University Press.

REINDL, Susanne,

(2004) *Computerstrafrecht im Überblick*, Wien: Facultas Verlags- und Buchhandels.

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

b) Os instrumentos internacionais e supranacionais

CAEIRO, Pedro,

(2012) «A jurisdição penal da União Europeia como meta-jurisdição: em especial, a competência para legislar sobre as bases de jurisdição nacionais», in: AA.VV., *Estudos em Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho*, vol. III, Coimbra: Coimbra Editora, pp. 179-210.

(2014) «A coerência dos sistemas penais nacionais em face do direito europeu», in: AA.VV., *O Espaço de Liberdade, Segurança e Justiça da EU – Desenvolvimentos Recentes* (org.: Constança Urbano de Sousa), Lisboa: Ediuial, 2014, pp. 241-255.

MITTAL, Sandeep, e SHARMA, Priyanka,

(2017) «A Review of International Legal Framework to Combat Cybercrime», *International Journal of Advanced Research in Computer Science*, pp. 1372-1374.



FACULDADE DE DIREITO
Universidade de Lisboa

c) A jurisprudência do TEDH

Robathin vs. Austria 2012.

Bernh Larsen Holding As vs. Norway 2013.

Sérvulo & Associados – Sociedade de Advogados, RL e Outros vs. Portugal 2015.

Trabajo Rueda vs. Spain 2017.

Ivashchenko vs. Russia 2018.

d) A jurisprudência do TJUE

Digital Rights Ireland (Casos C-293/12 e C-594/12).

Tele2 Sverige e Watson (Casos C-203/15 e C-698/1).

e) Os direitos estrangeiros e o direito comparado

AA.VV.

(2019) *Cybercrime* (org.: Alberto Cadoppi, Stefano Canestrari, Adelmo Manna e Michele Papa), Milano: UTET.

CUELLAR SERRANO, Nicolas González,

(2008) «Garantías constitucionales de la persecución penal en el entorno digital», in: AA.VV., *Prueba y Proceso Penal – Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado* (org.: Juan Luis Gómez Colomer), Valencia: Tirant lo Blanch.

FACCIOLA, John M., e BARRET, Lindsey,

(2016) «Law of the Foal: Careful Steps Towards Digital Competence in Proposed Rules 902(13) and 902(14)», *Georgetown Law Technology Review*, n.º 6, pp. 6-16.

FEHR, Colton,

(2018) «Digital Evidence and the Adversarial System: A Recipe for Disaster?», *Canadian Journal of Law & Technology*, vol. 16, n.º 2, pp. 443-468.

FORGÓ, Kikolaus, HAWELLEK, Christian, KNOKE, Friederike, e STOKLAS, Jonathan,

(2005) «The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings», in: AA.VV., *New Technology, Big Data and the Law* (org.: Marcelo Corrales, Mark Fenwick e Nikolaus Forgó), Singapore: Springer, 2017, pp. 251-280.

GLESS, Sabine, e MARTIN, Jeannine,

(2013) «The comparative method in European Courts: A comparison between the CJEU and EctH», *Bergen Journal of Criminal Law and Criminal Justice*, n.º 1, pp. 36-52.



FACULDADE DE DIREITO
Universidade de Lisboa

KERR, Orin S.,

- (2005) «Digital Evidence and the New Criminal Procedure», *Columbia Law Review*, vol. 105, n.º 279, pp. 443-468.
- (2015) «Search Warrants in an Era of Digital Evidence», *Mississippi Law Journal*, vol. 75, pp. 85-145.
- (2015) «Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data», *Texas Tech Law Review*, vol. 48, n.º 1, pp. 1-36.

ROSCINI, Marco,

- (2016) «Digital Evidence as a Method of Proof Before the International Court of Justice», *Journal of Conflict and Security Law* 21, pp. 541-554.

SCHUH, Daniel,

- (2012) *Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz*, Berlin: Duncker & Humblot.

f) A Lei do Cibercrime

ASCENSÃO, José de Oliveira,

- (2001) «Criminalidade Informática», in: AA.VV., *Direito da Sociedade da Informação*, vol. II, Coimbra Editora, pp. 203-228.
- (2012) «O cibercrime», in: AA.VV., *Direito Penal Económico e Financeiro – Conferências do Curso Pós-Graduado de Aperfeiçoamento* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Coimbra Editora, pp. 307-327.

VENÂNCIO, Pedro Dias,

- (2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

VERDELHO, Pedro,

- (2015) «Lei do Cibercrime», in: AA.VV., *Enciclopédia de Direito e Segurança* (coord. Jorge Bacelar Gouveia E Sofia Santos), Coimbra: Almedina, pp. 255-263.
- (2010) «Anotação à Lei n.º 109/2009, de 15 de setembro», in AA.VV., *Comentário das Leis Penais Extravagantes*, vol. I (org.: Paulo Pinto de Albuquerque e José Branco), Lisboa: Universidade Católica Editora.
- (2009) «A nova Lei do Cibercrime», *Scientia Iuridica* 320, pp. 717-749.

VERDELHO, Pedro, BRAVO, Rogério, e ROCHA, Manuel Lopes,

- (2003) *Leis do Cibercrime*, vol. 1, Lisboa: Centro Atlântico.

Título II - O CIBERCRIME

a) Os crimes informáticos da Lei do Cibercrime



FACULDADE DE DIREITO
Universidade de Lisboa

Ver o Título III, alíneas *a)* a *f)*.

b) Os crimes informáticos do Código Penal

Ver o Título III, alíneas *g)* e *h)*.

c) Os crimes cometidos por meio de um sistema informático

KING, T.C., AGGARWAL, N., TADDEO, M. et al.,

(2020) «Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions», *Sci Eng Ethics*, No. 26, pp. 89-120.

WIENER, Asaf,

(2015) «Virtual Crimes, Actual Threats: Detering National Security Offenses Committed Through Cyberspace», *Journal of Law and Cyber Warfare*, vol. 4, Issue 2, pp. 1-23.

d) Os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico

AA.VV.,

(2018) *Cibercriminalidade e Prova Digital – Jurisdição Penal e Processual Penal* (org.: CEJ), Lisboa: Coleção Formação Contínua (ebook).

Título III - OS CRIMES INFORMÁTICOS

a) A falsidade informática (art. 3.º LCib) vs. a falsificação de documento (art. 256.º CP)

MONIZ, Helena Isabel Gonçalves,

(1993) *O crime de falsificação de documentos – Da falsificação intelectual e da falsidade em documento*, Coimbra: Almedina.

NUNES, Duarte Alberto Rodrigues,

(2017) «O crime de falsidade informática», *Revista Julgar*^{online}, pp. 1-53. Publicação online (consultado em 10.02.2020).

VENÂNCIO, Pedro Dias,

(2010) «O crime de falsidade informática», *JusNet* 120. Publicação online: <http://jusjornal.wolterskluwer.pt>



FACULDADE DE DIREITO
Universidade de Lisboa

(consultado em 10.02.2020).

b) O dano relativo a programas e outros dados informáticos (art. 4.º LCib) vs. o crime de dano (art. 212.º CP)

NUNES, Duarte Alberto Rodrigues,

(2018) «O crime de dano relativo a programas ou outros dados informáticos», *Revista do Ministério Público*, n.º 153, pp. 141-165.

SALVADORI, Ivan,

(2014) «Los delitos de daños informáticos en el Código Penal italiano», *Derecho Penal Contemporáneo – Revista Internacional*, n.º 47, pp. 87-119.

c) A sabotagem informática (art. 5.º LCib) vs. o crime de dano em instalações e perturbação de serviços (art. 277.º/1 d) CP) e o crime de sabotagem (art. 329.º CP)

ASCENSÃO, José de Oliveira,

(2012) «O cibercrime», in: AA.VV., *Direito Penal Económico e Financeiro – Conferências do Curso Pós-Graduado de Aperfeiçoamento* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Coimbra Editora, pp. 307-327.

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

d) O acesso ilegítimo (art. 6.º LCib)

COLEMAN, Gabriella,

(2015) *Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous*, 1.ª reimp., London/New York: Verso (1.ª ed., 2014).

e) A interceptação ilegítima (art. 7.º LCib)

ASCENSÃO, José de Oliveira,

(2012) «O cibercrime», in: AA.VV., *Direito Penal Económico e Financeiro – Conferências do Curso Pós-Graduado de Aperfeiçoamento* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Coimbra Editora, pp. 307-327.

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.



FACULDADE DE DIREITO
Universidade de Lisboa

f) A reprodução ilegítima de programa protegido (art. 8.º LCib)

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

ASCENSÃO, José de Oliveira,

(2012) «O cibercrime», in: AA.VV., *Direito Penal Económico e Financeiro – Conferências do Curso Pós-Graduado de Aperfeiçoamento* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Coimbra Editora, pp. 307-327.

g) A burla informática (artigo 221.º CP) vs. a burla clássica (art. 217.º CP)

AA.VV.,

(1999) *Comentário Conimbricense do Código Penal* (org.: Jorge de Figueiredo Dias), Tomo II, Coimbra: Coimbra Editora.

ASCENSÃO, José de Oliveira,

(2012) «O cibercrime», in: AA.VV., *Direito Penal Económico e Financeiro – Conferências do Curso Pós-Graduado de Aperfeiçoamento* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Coimbra Editora, pp. 307-327.

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

h) A devassa por meio de informática (artigo 193.º CP)

AA.VV.,

(2012) *Comentário Conimbricense do Código Penal* (org.: Jorge de Figueiredo Dias), Tomo I, 2.ª ed., Coimbra: Coimbra Editora.

ALBUQUERQUE, Paulo Pinto de,

(2015) *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª ed., Lisboa: Universidade Católica Editora.

i) Os problemas do concurso de normas e de infrações

CORREIA, Eduardo Henriques da Silva,



FACULDADE DE DIREITO
Universidade de Lisboa

(1996) *A Teoria do Concurso em Direito Criminal*, 2.^a reimp., Coimbra: Almedina.

D'ALMEIDA, Luís Duarte,

(2004) *O «Concurso de Normas» em Direito Penal*, Coimbra: Almedina.

DIAS, Jorge de Figueiredo,

(2019) *Direito Penal – Parte Geral*, Tomo I (Questões Fundamentais, A Doutrina Geral do Crime), 3.^a ed., Coimbra: Gestlegal.

MOUTINHO, José Lobo,

(2005) *Da unidade à pluralidade dos crimes no Direito Penal Português*, Lisboa: Universidade Católica.

j) A responsabilidade penal das pessoas coletivas e equiparadas (art. 9.º LCib)

MENDES, Paulo de Sousa,

(2003) «A responsabilidade de pessoas coletivas no âmbito da criminalidade informática em Portugal», in: AA.VV., *Direito da Sociedade da Informação* (org.: José de Oliveira Ascensão), vol. IV, Coimbra: Coimbra Editora, pp. 385-404.

k) A perda de bens (art. 10.º LCib) e a perda alargada

CAEIRO, Pedro,

(2011) «Sentido e função do instituto da perda de vantagens relacionadas com o crime no confronto com outros meios de prevenção da criminalidade reditícia (em especial, os procedimentos de confisco *in rem* e a criminalização do enriquecimento 'ilícito')», *Revista Portuguesa de Ciência Criminal*, Ano 21, n.º 2, pp. 267-321, publicado também na *Revista Brasileira de Ciências Criminais*, Ano 21, n.º 100 (2013), pp. 453-501.

(2018) «O confisco numa perspectiva de política criminal europeia», in: AA.VV., *O Novo Regime de Recuperação de Ativos à Luz da Diretiva 2014/42/UE e da Lei que a Transpôs* (org.: Maria Raquel Desterro Ferreira, Elina Lopes Cardoso e João Conde Correia), Lisboa: INCM/Ministério Público, pp. 21-38.

SIMÕES, Euclides Dâmaso,

(2006) «Cooperação na recuperação de ativos: Da partilha à repatriação integral», *RMP* 105, p. 117 ss.

Título IV - A PROVA DIGITAL

a) O conceito e as especificidades da prova digital

RODRIGUES, Benjamim da Silva,



FACULDADE DE DIREITO
Universidade de Lisboa

(2011) *Da prova penal, t. IV – Da prova eletrónico-digital e da criminalidade informático-digital*, Lisboa: Rei dos Livros.

FANTINATTI, João Marcos,

(1988) *Segurança em informática – Metodologia e prática*, Campinas/SP: McGraw-Hill.

b) O quadro legal vigente entre o CPP, a Lei do Cibercrime e a Lei n.º 32/2008, de 17 de julho

CAIADO, Nuno,

(2014) «Vigilância eletrónica e prova: Estudo de um caso e algumas reflexões», in AA.VV., *Direito da investigação criminal e da prova* (org.: Maria Fernanda Palma, Augusto Silva Dias, Paulo de Sousa Mendes e Carlota Almeida), Coimbra: Almedina, pp. 237-253.

NUNES, Duarte Rodrigues,

(2018) *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Coimbra: Gestlegal.

c) A jurisprudência do TJUE em matéria de conservação de dados de tráfego

RAMALHO, David Silva, e COIMBRA, José Duarte,

(2015) «A declaração de invalidade da Diretiva 2006/24/CE: Presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, detecção e repressão de crimes graves», *O Direito* 147, pp. 997-1045.

d) A preservação expedita de dados (art. 12.º LCib)

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

e) A revelação expedita de dados de tráfego (art. 13.º LCib)

VENÂNCIO, Pedro Dias,

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

f) A injunção para apresentação ou concessão do acesso a dados (art. 14.º LCib)

VENÂNCIO, Pedro Dias,



FACULDADE DE DIREITO
Universidade de Lisboa

(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.

g) A pesquisa e apreensão de dados informáticos (arts. 15.º e 16.º LCib)

WARREN, Samuel D., BRANDEIS, Louis D.,

(1890) “The Right to Privacy”, *Harvard Law Review*, vol. 4, n.º 5., pp. 193-220.

CUELLAR SERRANO, Nicolas González,

(2008) «Garantías constitucionales de la persecución penal en el entorno digital», in: AA.VV., *Prueba y Proceso Penal – Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado* (org.: Juan Luis Gómez Colomer), Valencia: Tirant lo Blanch.

FORGÓ, Kikolaus, HAWELLEK, Christian, KNOKE, Friederike, e STOKLAS, Jonathan,

(2005) «The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings», AA.VV., *New Technology, Big Data and the Law* (org.: Marcelo Corrales, Mark Fenwick e Nikolaus Forgó), Singapore: Springer, 2017, pp. 251-280.

KERR, Orin S.,

(2015) «Search Warrants in an Era of Digital Evidence», *Mississippi Law Journal*, vol. 75, pp. 85-145.

(2015) «Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data», *Texas Tech Law Review*, vol. 48, n.º 1, pp. 1-36.

KOOPS, Bert-Jaap,

(2013) «Police investigations in Internet open sources: Procedural-law issues», *Computer Law & Security Review*, n.º 29, pp. 654-665.

PINHEIRO, Alexandre de Sousa,

(2015) *Privacy e protecção de dados pessoais – A construção dogmática do direito à identidade informacional*, Lisboa: AAFDL.

RAMALHO, David Silva,

(2013) «A investigação criminal na *Dark Web*», *C&R* 14/15, pp. 383-429.

(2014) «A recolha de prova penal em sistemas de computação em nuvem», *Revista de Direito Intelectual* 2, pp. 123-162.

RAMOS, Armando Dias,

(2017) *A prova digital em processo penal – O correio electrónico*, 2.ª ed., Lisboa: Chiado Editora.

SCHEINDLIN, Shira A., CAPRA, Daniel J.,

(2012) *Electronic Discovery and Digital Evidence – Cases and Materials*, Saint Paul, MN: Thomson Reuters.



FACULDADE DE DIREITO
Universidade de Lisboa

VERDELHO, Pedro,

- (2015) «Lei do Cibercrime», in: AA.VV., *Enciclopédia de Direito e Segurança* (coord. Jorge Bacelar Gouveia E Sofia Santos), Coimbra: Almedina, pp. 255-263.
- (2010) «Anotação à Lei n.º 109/2009, de 15 de setembro», in AA.VV., *Comentário das Leis Penais Excepcionais*, vol. I (org.: Paulo Pinto de Albuquerque e José Branco), Lisboa: Universidade Católica Editora.
- (2009) «A nova Lei do Cibercrime», *Scientia Iuridica* 320, pp. 717-749.
- (2008) «Técnica no novo C.P.P.: Exames, perícias e prova digital», *Revista do CEJ* 9, pp. 145-171.
- (2004) «A obtenção de prova do ambiente digital», *RMP* 99, pp.117-136.

h) A apreensão de correio electrónico e de registos de comunicações de natureza semelhante (art. 17.º LCib)

CARDOSO, Rui,

- (2018) «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX», *RMP* 153, pp. 167-214.

MESQUITA, Paulo Dá,

- (2010) «Prolegómenos sobre prova eletrónica e interceptação de telecomunicações no direito processual penal português – O Código e a Lei do Cibercrime», *Processo penal, prova e sistema judiciário*, Coimbra: Coimbra Editora, pp. 83-129.

NEVES, Rita Castanheira,

- (2011) *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e Respetivo Regime Jurídico do Correio Eletrónico enquanto Meio de Obtenção de Prova*, Coimbra: Coimbra Editora.

PINHEIRO, Alexandre de Sousa,

- (2015) *Privacy e protecção de dados pessoais – A construção dogmática do direito à identidade informacional*, Lisboa: AAFDL.

RAMOS, Armando Dias,

- (2017) *A prova digital em processo penal – O correio electrónico*, 2.ª ed., Lisboa: Chiado Editora.

i) A interceção de comunicações (art. 18.º LCib)

RAMALHO, David Silva,

- (2017) *Métodos Ocultos de Investigação em Ambiente Digital*, Coimbra: Almedina.



FACULDADE DE DIREITO
Universidade de Lisboa

j) As ações encobertas digitais (art. 19.º LCib)

MEIREIS, Manuel Augusto Alves,

(1999) *O regime das provas obtidas pelo agente provocador em processo penal*, Coimbra: Almedina.

k) A monitorização on-line e a falta de norma habilitante

CALAVITA, Oscar,

(2018) «L'odissea del Trojan Horse: Tra potenzialità tecniche e lacune normative», *Diritto Penale Contemporaneo* 11, pp. 45-76.

CAMALDO, Lucio,

(2019) «Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico», *Diritto Penale Contemporaneo*^{online}, pp. 1-18.

GROßMANN, Sven,

(2018) «Zur repressiven online-Durchsuchung», *Goltdammer's Archiv für Strafrecht*, n.º 8, pp. 439-456.

RAMALHO, David Silva,

(2013) «O uso de *malware* como meio de obtenção de prova em processo penal», *C&R* 16, pp. 195-243.

VACIAGO, Giuseppe, e RAMALHO, David Silva,

(2016) «Online searches and online surveillance: The use of trojans and other types of malware as means of obtaining evidence in criminal proceedings», *Digital Evidence and Electronic Signature Law Review* 13, pp. 88-96.

l) A investigação criminal na Dark Web

GHAPPOUR, Ahmed,

(2017) «Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web», *Stanford Law Review*, vol. 69, pp. 1075-1136.

RAMALHO, David Silva,

(2013) «A investigação criminal na *Dark Web*», *C&R* 14/15, pp. 383-429.

m) A utilização de armadilhas digitais

BRITO, Maria Beatriz,

(2018) *Novas Tecnologias e Legalidade da Prova em Processo Penal – Natureza e enquadramento do GPS como*



FACULDADE DE DIREITO
Universidade de Lisboa

método de obtenção de prova, Coimbra: Almedina.

HOLT, Thomas J., e BOSSLER, Adam M.,

(2016) *Cybercrime in Progress – Theory and Prevention of Technology-enabled Offenses*, New York: Routledge.

PENA, Sérgio,

(2013) «Os produtos da videovigilância como meio de prova em processo penal», *Revista do CEJ*, n.º 2, pp. 85-118.

SCAMBRAY, Joel, MCCLURE, Stuart, e KURTZ, George,

(2012) *Hacking Exposed – Network Security Secrets and Solutions*, 7.ª ed., USA: McGraw-Hill Osborne Media.

SPITZNER, Lance,

(2002) *Honeypots – Tracking Hackers*, Illinois, Addison Wesley.

n) A prova digital obtida por particulares e investigadores privados

ANDRADE, Manuel da Costa,

(1984) «Sobre a valoração, como meio de prova em Processo Penal, das gravações produzidas por particulares», in: AA.VV., *Estudos em homenagem ao Prof. Doutor Eduardo Correia*, vol. I, Coimbra: Universidade de Coimbra, pp. 545-622.

BARIN, Catiuce Ribas,

(2013) «A valoração das gravações de áudio», *Revista de Concorrência e Regulação*, Ano IV, n.º 16, pp. 245-294.

COSTA, José Neves da,

(2013) «Do aproveitamento em processo penal das provas ilicitamente obtidas por particulares», *Revista de Concorrência & Regulação*, n.º 16, pp. 295-344.

(2019) «Provas ilicitamente obtidas por particulares», in: AA.VV., *Prova Penal Teórica e Prática* (org.: Paulo de Sousa Mendes e Rui Soares Pereira), Coimbra: Almedina.

TÍTULO V – A CADEIA DE CUSTÓDIA DIGITAL

a) A cadeia de custódia e a validade da prova

PRADO, Geraldo,

(2019) *A cadeia de custódia da prova no processo penal*, São Paulo: Marcial Pons.

REID, Melanie,

(2018) «A CSI Story: The Past, Present, and Future of Crime Scene Collection and What Litigators Need to



FACULDADE DE DIREITO
Universidade de Lisboa

Know», *Wake Forest Journal of Law & Policy*, vol. 8, n.º 2, pp. 101-146.

b) O valor da privacidade defronte da recolha de prova digital (art. 8.º CEDH)

PINHEIRO, Alexandre de Sousa,

(2015) *Privacy e protecção de dados pessoais – A construção dogmática do direito à identidade informacional*, Lisboa: AAFDL.

c) A jurisprudência do TEDH

Robathin vs. Austria 2012.

Bernh Larsen Holding As vs. Norway 2013.

Sérvulo & Associados – Sociedade de Advogados, RL e Outros vs. Portugal 2015.

Trabajo Rueda vs. Spain 2017.

Ivashchenko vs. Russia 2018.

d) As Federal Guidelines for Searching and Seizing Computers do Departamento de Justiça norte-americano

BRENNER, S. W., e FREDERIKSEN, B. A.,

(2002) «Computer Searches and Seizures: Some Unresolved Issues», *Mich. Telecomm. Tech. L. Rev.*, vol. 39, n.º 8, pp. 39-114.

CLANCY, Thomas K.,

(2005) «The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer», *Mississippi Law Journal*, n.º 75, pp. 193-286.

e) A jurisprudência norte-americana

United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

State v. Schroeder, 613N.W.2d911 (Wis. App. 2000).

United States v Ivanov No. 300CR00183AWT. 2001.

United States v. Wey, ___ F. Supp. 3d ___, 2017 WL 2574026 (S.D.N.Y. June 14, 2017) (decision granting suppression).

f) A Plain View Doctrine e a Cyberplain View



FACULDADE DE DIREITO
Universidade de Lisboa

CHANG, Ray Ming,

(2007) «Why the Plain View Doctrine Should Not Apply to Digital Evidence», *Suffolk Journal of Trial and Appellate Advocacy*, vol. 12, pp. 31-67.

MOORE, Robert,

(2004) «To view or not to view: Examining the plain view doctrine and digital evidence», *American Journal of Criminal Justice*, vol. 29, n.º 1, pp. 57-73.

PRICE, Michael W.,

(2016) «Rethinking Privacy: Fourth Amendment ‘Papers’ and the Third-Party Doctrine», *Journal Of National Security Law & Policy*, vol. 8, pp. 247-299.

TÍTULO V - A COOPERAÇÃO JUDICIÁRIA INTERNACIONAL

a) O acesso unilateral a dados armazenados em sistemas informáticos localizados no estrangeiro

BACHMAIER WINTER, Lorena,

(2017) «Remote computer searches under Spanish Law: The proportionality principle and the protection of privacy», *ZStW*, 129(1), pp. 205-231.

PEREIRA, Rui Soares,

(2019) «O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticos localizados no estrangeiro», *Revista de Estudos Europeos*, N.º extraordinário monográfico, 1, pp. 246-273.

RAMALHO, David Silva,

(2014) «A recolha de prova penal em sistemas de computação em nuvem», *Revista de Direito Intelectual*, n.º 2, pp. 123-162.

(2018) «A recolha de prova digital através de pesquisas informáticas transfronteiriças», in: AA.VV., *O domínio do imaterial – Prova digital, cibercrime e a tutela penal de direitos intelectuais* (org.: CEJ), ebook, pp. 55-69.

SVANTESSON, Dan Jerker B.,

(2016) «Law enforcement access to evidence via direct contact with cloud providers: Identifying the contours of a solution», *Comput. Law Secur. Rev.*, n.º 32, pp. 671-682.

b) O âmbito da cooperação judiciária internacional

GLESS, Sabine,

(2010) «Truth or due process? The use of illegally gathered evidence in the criminal trial», in: AA.VV., *German*



FACULDADE DE DIREITO
Universidade de Lisboa

national reports to the 18th International Congress of Comparative Law: Washington 2010 (org.: Jürgen Basedow, Uwe Kischel e Ulrich Sieber), Tübingen: Mohr Siebeck, pp. 675-709.

(2013) «Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle», *Utrecht Law Review*, n.º 4, pp. 90-108.

(2018) «Protecting Human Rights through Exclusionary Rules? Highlights on a Conflict in Criminal Proceedings from a Comparative Perspective», in: AA.VV., *Justice Without Borders – Essays in Honour of Wolfgang Schombourg* (org.: Martin Böse et. al.), Leiden/Boston: Brill/Nijhoff, pp. 159-179.

GLESS, Sabine, e VERVAELE, John A. E.,

(2013) «Law Should Govern: Aspiring General Principles for Transnational Criminal Justice», *Utrecht Law Review*, n.º 4, pp. 1-10.

MIFSUD BONNICI, Jeanne Pia, TUDORICA, Melania, e CANNATACI, Joseph A.,

(2018) «The European Legal Framework on Electronic Evidence», in: AA.VV., *Handling and Exchanging Electronic Evidence Across Europe* (org.: M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci e F. Turchi), pp. 189-235.

RAMOS, Vânia Costa,

(2014) «Introdução aos problemas da obtenção de prova em contexto transnacional e à proposta da instituição de uma decisão europeia de investigação», in: AA.VV., *Direito da Investigação Criminal e da Prova* (org.: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes), Coimbra: Almedina, pp. 323-363.

(2017) «Novos problemas em matéria de proibições de prova – A dimensão internacional – Regras de exclusão da prova obtida em violação da Convenção Europeia dos Direitos Humanos na Jurisprudência do Tribunal Europeu dos Direitos Humanos», in: AA.VV., *Estudos em Homenagem ao Professor Doutor Manuel da Costa Andrade* (org.: José Faria Costa et. al.), vol. II, Coimbra: Instituto Jurídico, pp. 739-773.

THAMAN, Stephen C.,

(2013) «Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules», in: AA.VV., *Exclusionary Rules in Comparative Law* (org.: Stephen C. Thaman), Dordrecht: Springer, pp. 403-446.

WADE, Marianne,

(2013) «General Principles of Transnationalised Criminal Justice? – Exploratory Reflections», *Utrecht Law Review*, n.º 4, pp. 165-183.

TÍTULO VI - A INTELIGÊNCIA ARTIFICIAL APLICADA AO DIREITO

a) Os sistemas periciais de auxílio à decisão judicial

BRITO, Susana de,

(1991) «Uma experiência do Projeto Normlog: O sistema do reenvio concebido para apoio ao ensino», in: AA.VV., *Colóquio Informática e Tribunais, Bases de Dados Administrativas e Jurídicas* (org.: Gabinete do Diretor da Informatização Judiciária), Lisboa: Ministério da Justiça, pp. 529-542.



FACULDADE DE DIREITO
Universidade de Lisboa

HESPANHA, António Manuel,

(2000) «Os juristas que se cuidem... Dez anos de inteligência artificial e Direito», *Themis*, ano I, n.º 1, pp. 139-169.

JENKINS, Johnathan,

(2008) «What Can Information Technology Do for Law? », *Harvard Journal for Law and Technology*, vol. 21, n.º 2, pp. 589-607.

STRANIERI, Andrew, e ZELEZNIKOW, John,

(2010) *Knowledge Discovery from Legal Databases*, Dordrecht, Netherlands: Springer.

SUSSKIND, Richard,

(1989) *Expert Systems in Law*, 1.ª ed. pbck, Oxford: Clarendon Press (1.ª ed., 1987).

(2008) *The End of Lawyers? Rethinking the Nature of Legal Services*, Oxford: Oxford University Press.

(2017) *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford: Oxford University Press.

(2017) *Tomorrow's Lawyers: An Introduction To Your Future*, Oxford: Oxford University Press.

(2019) *Online Courts and the Future of Justice*, Oxford: Oxford University Press.

TISCORNIA, Daniela,

(2014) «About 'Good Law?'», in: AA.VV., *Zeichen und Zauber des Rechts – Festschrift für Friedrich Lachmayer* (org.: E. Schweighofer et al.), Bern: Weblaw, pp. 437-449.

b) A representação e a formalização do conhecimento jurídico

AA.VV.,

(2019) *Formalising Jurisprudence – Festschrift for Hajime Yoshino* (org.: Friedrich Lachmayer, Erich Schweighofer, Michal Araszkiwicz e Marijan Pavcnik), Bern: Weblaw.

ARAÚJO, Fernando,

(1999) «Lógica jurídica e informática jurídica: Da axiomatização deontica às estruturas não-monotónicas do raciocínio rebatível», in: AA.VV., *Direito da Sociedade de Informação*, vol. I, Coimbra: Coimbra Editora, pp. 7-71.

BAYAMLIOĞLU, Emre, e Ronald LEENES, Ronald,

(2018) «The 'rule of law' implications of data-driven decision-making: a techno-regulatory perspective», *Journal Law, Innovation and Technology*, vol. 10, Issue 2, pp. 295-313.

PHILIPPS, Lothar,

(1994) «Artificial Morality and Artificial Law», *Artificial Intelligence and Law*, n.º 2, pp. 51-63.



FACULDADE DE DIREITO
Universidade de Lisboa

c) Os Big Data e a investigação criminal

BARRY, Nicholas,

(2013) «Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and A Computer-Utilizing Predictive-Coding Technology», *Vand. J. Ent. & Tech. L.*, vol 15, n.º 2, pp. 343-373.

DEVINS, Caryn, FELIN, Teppo, KAUFFMAN, Stuart, e KOPPL, Roger,

«The Law and Big Data», *Cornell Journal of Law and Public Policy*, vol. 27, n.º 2, pp. 357-413.

FERGUSON, Andrew Guthrie,

(2020) «Big Data Prosecution & Brady», *UCLA Law Review* (Forthcoming), pp. 1-71.

GOODMAN, Aaron,

(2016) «Predictive Coding: A Better Way to Deal with Electronically Stored Information», *Litigation*, vol. 43, n.º 1, pp. 1-5.

ZAVRŠNIK, Aleš,

(2019) «Algorithmic justice: Algorithms and big data in criminal justice settings», *European Journal of Criminology*, n.º 18.

Online: <https://journals.sagepub.com/doi/10.1177/1477370819876762> (consultado em 05.02.2020).

d) Os sistemas de apoio à mineração de dados relevantes para a questão de facto

AA.VV.,

(2013) *Privacy, Due Process and the Computational Turn – The Philosophy of Law Meets the Philosophy of Technology* (Mireille Hildebrandt e Katja de Vries), New York: Routledge.

ASHLEY, Kevin D.,

(2017) *Artificial Intelligence and Legal Analytics – New Tools for Law Practice in the Digital Age*, Cambridge: Cambridge University Press.

RON SIN, Xavier, e LAMPOS, Vasileios,

(2018) «In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data» (Appendix I), in: *European Charter on the Use of AI in Judicial Systems*, pp. 13-61.
Online: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (consultado em 05.02.2020).



FACULDADE DE DIREITO
Universidade de Lisboa

e) Os sistemas de apoio à motivação da questão de direito

AA.VV.,

(2013) *Human Law and Computer Law: Comparative Perspectives* (org.: Mireille Hildebrandt e Jeanne Gaakeer), Dordrecht, Netherlands: Springer.

HILDEBRANDT, Mireille,

(2015) *Smart Technologies and the End(s) of Law – Novel Entanglements of Law and Technology*, Cheltenham, UK: Edward Elgar.

f) Os sistemas automáticos de decisão judicial e o problema do juiz-robô

AA.VV.,

(2016) *Robot Law* (org.: Ryan Calo, Michael Froomkin e Ian Kerr), Cheltenham, UK: Edward Elgar.

(2020) *Inteligência Artificial & Direito* (org.: Manuel Lopes Rocha e Rui Soares Pereira), Coimbra: Almedina.

BASILE, Fabio,

(2019) «Intelligenza artificiale e diritto penale: Quattro possibili percorsi di indagine», *Diritto Penale e Uomo*, pp. 1-33.

GIALUZ, Mitja,

(2019) «Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed europa», *Diritto Penale Contemporaneo*^{online}, pp. 1-23.

HILDEBRANDT, Mireille,

(2018) «Algorithmic Regulation and the Rule of Law», *Philosophical Transactions of the Royal Society A*, vol. 376, Issue 2128, p. 376 ss.

PARODI, Cesare, e SELLAROLI, Valentina,

(2019) «Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco», *Diritto Penale Contemporaneo*^{online}, 6, pp. 47-71.

TÍTULO VII – OS AGENTES INTELIGENTES E A RESPONSABILIDADE

a) As máquinas e a responsabilidade

PALMA, Maria Fernanda,



FACULDADE DE DIREITO
Universidade de Lisboa

(2014) «O Direito como máquina jurídica e o controlo de si mesmo como fundamento da responsabilidade»,
Revista Portuguesa de Filosofia, vol. 70, n.º 4, pp. 681-694.

b) Os veículos autónomos e o direito penal

AA.VV.,

(2019) *Veículos autónomos e direito penal* (org.: Heloísa Estelitta e Alaor Leite), São Paulo: Marcial Pons.

NOTA: este mapa é preenchido tantas vezes quantas as necessárias para descrever as diferentes unidades curriculares.