FACULDADE DE DIREITO
Universidade de Lisboa

DIREITO PENAL IV - CIBERCRIMES

(2014/2015)

Prof. Doutor Miguel Prata Roque

FICHA CURRICULAR / ACADEMIC ABSTRACT

TEMA: O Cibercrime Enquanto Fenómeno de Desterritorialização das Infrações Penais

SUMÁRIO: «Direito Penal IV» utilizará o estudo do regime dos cibercrimes como pretexto para enfrentar novos problemas decorrentes da globalização jurídica e do progresso tecnológico, que conduziram a uma crescente desmaterialização e desterritorialização das atuações criminosas. Para além disso, essa constante evolução tecnológica transporta consigo o risco de tornar obsoletos os tipos de crimes previstos para incriminar as atuações cibernéticas ilícitas, o que exige da ciência jurídica uma nova equação dos limites do princípio da legalidade penal. Ao longo do semestre letivo, estudar-se-ão não só os aspetos mais relevantes da Teoria Geral do Crime, quando aplicada aos cibercrimes, como se procederá a um estudo detalhado das várias tipologias de cibercrimes; sejam eles cibercrimes em sentido estrito – isto é, aqueles que resultam de expressa previsão típica, dirigida à proteção do bem jurídico específico da inviolabilidade dos sistemas informáticos –, sejam eles em sentido amplo – o que compreende, igualmente, os crimes comuns praticados por meio informático. Outro aspeto central corresponde ao estudo dos meios de investigação criminal em meio digital.

I. PROGRAMA

PARTE I

TEORIA GERAL DOS CIBERCRIMES E DIREITO PENAL TRANSNACIONAL

1. A dimensão transnacional do Direito Penal

    1.1. A globalização e a reação das ordens jurídicas nacionais
    1.2. Desmaterialização do crime: inovação tecnológica dos cibercrimes
    1.3. Decadência do princípio da territorialidade e aplicação de Direito Penal estrangeiro, internacional e transnacional
    1.4. Fontes transnacionais de Direito Penal – em especial, a Convenção Europeia do Cibercrime
    1.5. A determinação da lei penal aplicável aos cibercrimes

2. A diversidade de bens jurídicos protegidos pelos cibercrimes

    2.1. A consagração constitucional de bens jurídicos pessoais
    2.2. Em especial, o direito à inviolabilidade das comunicações
    2.3. Em especial, o direito à inviolabilidade dos sistemas informáticos
    2.4. A resolução de situações de conflito entre direitos fundamentais

3. O princípio da legalidade penal e a sua compressão pelo progresso tecnológico e científico

    3.1. O fundamento constitucional do princípio da legalidade penal
    3.2. O contínuo desfasamento entre os tipos de cibercrimes e a realidade tecnológica e científica
    3.3. Adaptação ao progresso tecnológico e interpretação atualista
    3.4. As normas penais em branco

4. Causas de exclusão da ilicitude e da culpa

    4.1. Especificidades da justificação e da exculpação nos cibercrimes
    4.2. O exercício de um direito: em especial, a liberdade de expressão, a liberdade de imprensa e a investigação criminal
    4.3. O problema do consentimento e do acordo – a renúncia de direitos fundamentais pelo (potencial) ofendido

5. Comparticipação e responsabilidade penal das pessoas coletivas

    5.1. Especificidades de regimes de comparticipação quanto à prática de cibercrimes
    5.2. A responsabilidade penal das pessoas coletivas
    5.3. A responsabilidade penal individual dos dirigentes
    5.4. Problemas de cumulação de sanções e a proibição de *"bis in idem"*

6. As consequências dos cibercrimes

    6.1. A medida da pena e a sua fixação
    6.2. As sanções acessórias
    6.3. Em especial, a perda de bens obtidos pela prática de cibercrimes

PARTE II

A TIPOLOGIA DE CIBERCRIMES

7. A distinção entre cibercrimes em sentido estrito e cibercrimes em sentido amplo

    7.1. A noção ampla de cibercrimes: inclusão dos crimes comuns praticados por meio informático
    7.2. Especificidade dos crimes comuns praticados por meio informático
    7.3. Os cibercrimes em sentido estrito: os crimes informáticos

7.4. A multiplicação de fontes normativas de incriminação

8. Tipos especiais de cibercrimes (ou de crimes informáticos)

8.1. A falsidade informática
8.2. A burla informática
8.3. O dano relativo a programas e outros dados informáticos
8.4. A sabotagem informática
8.5. O acesso ilegítimo
8.6. A interceção ilegítima
8.7. A reprodução ilegítima do programa protegido

9. Tipos comuns de cibercrimes (ou de crimes praticados por meio informático)

9.1. Consequências da prática de crimes comuns por meio informático
9.2. O caso particular dos crimes contra a honra
9.3. Problemas de distinção e de concurso entre crimes comuns praticados por meio informático e cibercrimes em sentido estrito

PARTE III
O REGIME PROCESSUAL PENAL APLICÁVEL AOS CIBERCRIMES

10. Âmbito de aplicação e relações de subsidiariedade

10.1. Os crimes abrangidos pelo regime processual penal especial
10.2. A aplicação subsidiária da lei processual penal geral
10.3. A aplicação subsidiária do regime das comunicações eletrónicas
10.4. A aplicação subsidiária do regime dos dados pessoais
10.5. A aplicação subsidiária da lei procedimental administrativa (às operações policiais preventivas ou de sanção não penal)

11. As medidas cautelares de preservação e conservação de prova

    11.1. A preservação expedita de dados
    11.2. O acesso expedito a dados de tráfego
    11.3. Em especial, a localização celular
    11.4. Aplicação subsidiária da lei processual penal geral

12. Os meios de obtenção de prova digital

    12.1. Acesso jurisdicionalmente autorizado a dados informáticos
    12.2. A pesquisa de dados informáticos: buscas e revistas
    12.3. A apreensão de dados informáticos – diversidade de regimes
        12.3.1. O problema da apreensão do correio eletrónico
        12.3.2. A apreensão de dados armazenados em sistemas informáticos
        12.3.3. A afetação de outros direitos fundamentais: reserva da intimidade privada, segredo profissional, segredo comercial, etc.
        12.3.4. O consentimento presumido
    12.4. A interceção de comunicações eletrónicas em curso e o paralelismo com as escutas telefónicas

13. O uso de meios encobertos ou tipicamente ilícitos para efeitos de investigação criminal

    13.1. A investigação criminal na *"Dark Web"*
    13.2. O uso de *"malware"* e de outros meios informáticos (usualmente) ilícitos para efeitos de investigação criminal
    13.3. O problema da provocação dos suspeitos de cibercrimes
    13.4. As ações encobertas de investigação

PARTE IV

A COOPERAÇÃO ADMINISTRATIVA E JUDICIÁRIA INTERNACIONAL EM MATÉRIA DE CIBERCRIMES

14. A globalização e o reforço da cooperação internacional

14.1. Métodos interestaduais
14.2. Métodos de cooperação em rede
14.3. Em especial, a INTERPOL e os *"red flag alerts"*: o problema do controlo jurisdicional

15. O procedimento transnacional de cooperação administrativa e judiciária

15.1. Tramitação procedimental
15.2. O interesse público do Estado requisitado: princípio de dupla incriminação e motivos de recusa
15.3. O acesso a dados informáticos armazenados ou conservados por autoridade estrangeira ou internacional
15.4. A interceção transnacional de comunicações eletrónicas
15.5. Especificidades das ações extraterritoriais de *"intelligence"*
15.6. A responsabilidade civil internacional por ofensa de direitos fundamentais dos suspeitos

II. REGIME DE AVALIAÇÃO

De acordo com a alínea *b)* do artigo 3º do Regulamento de Avaliação de Conhecimentos nos Cursos de Especialização Integrados nos Mestrados de Bolonha, que pode ser consultado *in* http://www.fd.ulisboa.pt/LinkClick.aspx?fileticket=_h0aqv1zibs%3d&tabid=184) , o regime de avaliação será o seguinte:

- Avaliação de participações orais em aula: 30%
- Trabalho escrito de investigação sobre um tema do programa: 70%

O trabalho escrito deve ser entregue até 30 de abril de 2015, seguindo os seguintes requisitos:

a) Máximo de 50 páginas (excluindo a bibliografias e eventuais anexos);
b) Comunicação ao Regente do tema do trabalho, para aprovação, até 6 de março de 2015;
c) Escrito em português;
d) Entrega de uma declaração de autenticidade assinada.

A avaliação será pessoalmente notificada aos alunos até à penúltima semana do calendário escolar. Os alunos cujas notas sejam negativas (9 ou menos valores) e os alunos cujas notas sejam superiores a 15 valores serão submetidos a uma avaliação oral, de acordo com as seguintes regras:

a) Duração máxima de 15 minutos, por aluno;
b) Discussão exclusivamente centrada no tema do trabalho escrito;
c) Avaliação oral durante o horário de aula, na última semana do semestre.

Os alunos reprovados na época normal podem apresentar-se à época de recurso, nos termos do n.º 1 do artigo 7º do Regulamento de Avaliação. O recurso será composto por uma prova oral.

III. BIBLIOGRAFIA

<u>Portuguesa</u>

- ANA PAULA RODRIGUES, *Pornografia de menores: novos desafios na investigação e recolha de prova digital*, *in* «Revista do CEJ», 15 (2011), 261-291
- BRUTO DA COSTA / ROGÉRIO BRAVO, *Spam e Mail bombing – Subsídios para uma Perspectiva Criminal*, Quid Iuris, 2005

- CRISTINA MÁXIMO DOS SANTOS, *As novas tecnologias da informação e o sigilo das telecomunicações*, *in* «Revista do Ministério Público», 99 (2004), 89-116

- GARCIA MARQUES / LOURENÇO MARTINS, *Direito da Informática*, 2.ª edição refundida e atualizada, Almedina, 2006

- DAVID SILVA RAMALHO, *A investigação criminal na Dark Web*, *in* «Concorrência & Regulação», n.º 14/15 (2013), 383-430

- DAVID SILVA RAMALHO, *O uso de malware como meio de obtenção de prova em processo penal*, *in* «Concorrência & Regulação», n.º 14/15 (2013),

- INÊS FERREIRA LEITE, *O Conflito de Leis Penais – Natureza e Função do Direito Penal Internacional*, Coimbra Editora, 2008

- JOÃO BARBOSA DE MACEDO, *Algumas Considerações Acerca dos Crimes Informáticos em Portugal*, *in* «Direito Penal Hoje – Novos Desafios e Novas Respostas», Coimbra Editora, 2009, 221-262

- JOSÉ DE OLIVEIRA ASCENSÃO, *Criminalidade Informática*, *in* «Direito da Sociedade da Informação», Volume II, Coimbra Editora, 2001, 203-227

- MARIA DA GLÓRIA LEITÃO, *A Admissibilidade como meio de prova em processo disciplinar das mensagens de correio eletrónico enviadas e recebidas por trabalhador a partir de e na caixa de correio fornecida pela entidade empregadora*, Colóquio no STJ, Lisboa, 10 outubro de 2012, disponível *in* http://www.stj.pt/ficheiros/coloquios/coloquios_STJ/V_Coloquio/maria_glria_leito.pdf

- PAULO SOUSA MENDES, *A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal*, *in* «Direito da Sociedade da Informação» (org. José de Oliveira Ascensão), Vol. IV, Coimbra Editora, 2003, 385-404

- PEDRO CAEIRO, *Fundamento, Conteúdo e Limites da Jurisdição Penal do Estado*, Coimbra Editora, 2010

- PEDRO VENÂNCIO, *Investigação e Meios de Prova na Criminalidade Informática*, Verbo Jurídico, 2006

- PEDRO VENÂNCIO, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2011

- PEDRO VERDELHO, *Cibercrime*, *in* Direito da Sociedade da Informação, *in* «Direito da Sociedade da Informação» (org. José de Oliveira Ascensão), Vol. IV, Coimbra Editora, 347-373

- PEDRO VERDELHO, *A obtenção de prova no ambiente digital*, *in* «Revista do

Ministério Público», 99 (2004), 117-136

- PEDRO VERDELHO, *A nova Lei do Cibercrime*, *in* «Scientia Ivridica», 320 (2009), 717-749

- PEDRO VERDELHO, *Phishing e outras formas de defraudação nas redes de comunicação*, *in* «Direito da Sociedade da Informação» (org. José de Oliveira Ascensão), Vol. IV, Coimbra Editora, 2003, Volume VIII, Coimbra Editora, 2009, 407-420

- RENATO LOPES MILITÃO, *A propósito da Prova Digital no Processo Penal*, *in* «Revista da Ordem dos Advogados», Ano 72, jan/mar (2012), 247-285

- RITA CASTANHEIRA NEVES, *As ingerências nas comunicações electrónicas em protecção penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra editora, 2011

- ROGÉRIO BRAVO, *Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta*, *in* «Polícia e Justiça», 7 (2006), 207-216

- VÂNIA COSTA RAMOS, *Âmbito e extensão do Segredo das telecomunicações. Breves notas ao Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, de 2 de Março de 2006*, *in* «Revista do Ministério Público», 112 (2007), 141-159

Estrangeira

- ANGELA ADRIAN, *Could A Small Town in Romania bring Australia to its Cyber-knees? Not if They Accede to the EU Convention on Cybercrime*, *in* «Journal of International Commercial Law and Technology», Vol. 7, n.º 4, 2012, 328-338

- BERT-JAAP KOOPS, *Police Investigations in Internet open sources: Procedural-law issues*, *in* «Computer Law & Security Review», 29 (2013), 654-665

- CARLOS ROMEO CASABONA, *De los Delitos Informáticos al Cibercrimen. Una Aproximación Conceptual y Político-Criminal*, *in* «El Cibercrimen: Nuevos Retos Jurídico-Penales, Nuevas Respuestas Político-Criminales», Editorial Comares, 2006

- CÉDRIC J. MAGNIN, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?*, Santa Clara University, June 2001 (*in* http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf)

- GIOVANNI BUONOMO, *Le Responsabilità Penali*, *in* «Diritto dell'Informatica», Giuffrè Editore, 1999

- JOACHIM VOGEL, *Towards a Global Convention against Cybercrime* (First World Conference of Penal Law – Penal Law in the XXIst Century – Mexico – Guadalajar, 18-23 November, 2007), *in* ReAIDP / e-RIAPL, 2008, C-07, 1-20 (*in* http://www.penal.org/IMG/Guadalajara-Vogel.pdf)

- MIKA HAYASHI, *Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace*, *in* «Law», 6 (2006), 284-302

- MIKE KEYSER, *The Council of Europe Convention on Cybercrime*, *in* «Journal of International Law & Politics», Vol. 12, n.º 2, Spring 2003, 287-326 (*in* http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf)

- MIRIAM F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, *in* «Journal of Computer and Information Law», Vol. 43, n.º 2, 2005, 329-362 (*in* http://repository.jmls.edu/cgi/viewcontent.cgi?article=1057&context=jitpl)

- MOLLY VAN HOUWELING, *Enforcement of foreign judgements, the first amendment, and internet speech: notes for the next «Yahoo! V. Licra»"*, *in* «Michigan Journal of International Law», 3 (2003), 697-717

- NANCY E. MARION, *The Council of Europe´s Cyber Crime Treaty: An exercise in Symbolic Legislation*, *in* «International Journal of Cyber Criminology», Vol. 4, n.ºs 1-2, 2010, 699-712 (*in* http://www.cybercrimejournal.com/marion2010ijcc.pdf)

- RAINER SCHRÖDER, *Globalisierung des Internetrechts*, *in* «Rechtstheorie», 39 (2008), 231-253

- SARA L. MARLER, *The Convention on Cyber-Crime: Should the United States Ratify?*, *in* «New England Law Review», Vol. 37, n.º 1, 2002, 183-219 (*in* http://www.nesl.edu/userfiles/file/lawreview/vol37/1/marler.pdf)

- SHANNON L. HOPKINS, *Cybercrime Convention: a positive beginning to a long road ahead*, *in* «Journal of High Technology Law», Vol. 2, n.º 1, 2003, 101-121

- SHANNON L. HOPKINS, *Cybercrime Convention: a positive beginning to a long road ahead*, *in* «Journal of High Technology Law», Vol. 2, n.º 1, 2003, 101-121 (*in* http://www.suffolk.edu/documents/jhtl_publications/SHOPKINSV2N1N.pdf)

- ULRICH SIEBER, *Internationales Strafrecht im Internet – Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace*, *in* «NJW», 1999, 2067-2068