FACULDADE DE DIREITO
Universidade de Lisboa

FICHA DE UNIDADE CURRICULAR
DIREITO PENAL V - TURMA A/NOITE

Mestrado em Direito e Prática Jurídica – Especialidade: Direito Penal
Mestrado em Segurança da Informação e Direito no Ciberespaço – Protocolo com o Instituto Superior Técnico e a Escola Naval

2023/2024
2.º Semestre

Unidade curricular

Direito Penal V – *Cibercrime e prova digital*

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

Teresa Quintela de Brito – 2 horas

Outros docentes e respectivas cargas letivas na unidade curricular

Não aplicável

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

A Lei n.º 109/09 (Lei do Cibercrime) transpôs para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI, do Conselho, relativa a ataques contra sistemas de informação e adaptou o Direito interno à Convenção sobre Cibercrime (Budapeste, 23.11.2001). São objectivos do presente curso fornecer uma visão pormenorizada e crítica da Lei do Cibercrime, quer no plano substantivo (crimes informáticos), quer no plano adjectivo (normas processuais e probatórias), procurando articulá-la com instrumentos jurídicos internacionais, de Direito da União Europeia, o Código Penal, o Código de Processo Penal e outros diplomas legislativos nacionais.

Conteúdos programáticos

PARTE I – APRESENTAÇÃO DA DISCIPLINA

1. O programa
2. Os instrumentos internacionais, maxime, a Convenção sobre o Cibercrime, o 1.º Protocolo Adicional relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos (Estrasburgo, 28.01.2003) e o 2.º Protocolo Adicional relativo ao reforço da cooperação e da comunicação de provas eletrónicas (Estrasburgo, 28.05.2022).
3. Os instrumentos supranacionais, maxime Directivas UE.
4. A jurisprudência do TEDH
5. A jurisprudência do TJUE
6. Os direitos estrangeiros e o direito comparado
7. A Lei do Cibercrime (LCib) e principais diplomas legislativos nacionais com os quais tem de articular-se
   7.1. *No plano processual:* Código de Processo Penal; Leis n.os 32/2008 e 41/2004 quanto aos dados de tráfego e de localização; Leis n.os 101/2001 (acções encobertas) quanto aos meios de obtenção de prova; Lei n.º 88/2017 (Decisão Europeia de Investigação em matéria penal) e Lei n.º 59/2019 (dados pessoais para prevenção, detecção, investigação ou repressão de infracções penais) quando à cooperação judiciária internacional.
   7.2. No plano substantivo: Código Penal; Lei n.º 58/2019 (Lei de protecção de dados pessoais).
   7.3. No plano da Cibersegurança: Lei n.º 46/2018 (Regime jurídico da segurança no ciberespaço)
8. Notas práticas do Gabinete do Cibercrime com referências jurisprudenciais a crimes informáticos e à prova digital.

PARTE II – O CIBERCRIME

1. Os crimes informáticos da Lei do Cibercrime (arts. 3.º-8.º, da Lei n.º 109/2009, por último alterada pela Lei n.º 79/2021, de 24.11, que introduziu novas incriminações e alterou os respectivos arts. 3.º e 6.º, bem como o

Código Penal).

2. Os crimes informáticos do Código Penal (*v.g.* burla informática e nas comunicações; aliciamento de menores para fins sexuais por meio de tecnologias de informação e comunicação – arts. 221.º e 176.º-A do CP)

3. Os crimes cometidos por meio de um sistema informático (*v.g.* ciberperseguição; injúrias através das redes sociais (calúnia); pornografia de menores; abuso de cartão, dispositivo ou dados de pagamento; devassa da vida privada; gravações e fotografias ilícitas – arts. 154.º-A, 183.º/1, al. a), ou 2, 176.º, 225º, 192.º e 199.º do CP).

4. Os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (cfr. art. 11.º/1, da LCib).

PARTE III – OS CRIMES INFORMÁTICOS EM ESPECIAL; PROBLEMAS DE CONCURSO DE NORMAS E DE CONCURSO DE INFRAÇÕES

1. Falsidade informática (art. 3.º da LCib)
   1.1. Falsidade informática *vs.* falsificação de documento (art. 256.º do CP),
   1.2. Falsificação informática (art. 3.º/1 e 2 da LCib) *vs*. contrafação de cartões ou outros dispositivos de pagamento (art. 3.º-A LCib)
   1.3. Uso de cartões ou outros dispositivos de pagamento contrafeitos (art. 3.º-B da LCib) *vs.* burla informática (art. 221º do CP) *vs*. abuso de cartão, dispositivo ou dados de pagamento (art. 225.º do CP).
   1.4. Uso de dispositivo contrafeito que permita acesso a sistema de comunicações ou a serviço de acesso condicionado (art. 3.º/3 LCib) *vs.* burla nas comunicações (art. 221.º/2 do CP)

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

3. Sabotagem informática (art. 5.º da LCib) *vs*. burla nas comunicações (art. 221.º/2 do CP)

4. Acesso ilegítimo (art. 6.º LCib) *vs.* dano informático (art. 4.º da LCib)

5. Interceção ilegítima (art. 7.º da LCib) *vs.* dano informático (art. 4.º da LCib)

6. Burla informática (artigo 221.º/1 do CP) *vs.* burla clássica (art. 217.º do CP)

PARTE IV – A PROVA DIGITAL

1. Conceito e especificidades da prova digital

2. Quadro legal vigente: entre o Código de Processo Penal, a Lei do Cibercrime, a Lei n.º 32/2008, a Lei n.º 41/2004 e a Lei n.º 59/2019

3. Jurisprudência do TJUE e do Tribunal Constitucional português sobre conservação massiva de dados de tráfego e de localização

4. Meios cautelares de preservação da prova
   4.1. Preservação expedita de dados (art. 12.º da LCib)
   4.2. Revelação expedita de dados de tráfego (art. 13.º do LCib)

5. Meios de obtenção de prova previstos na Lei do Cibercrime
   5.1. Injunção para apresentação ou concessão do acesso a dados (art. 14.º, máxime n.º 4, da LCib, *vs.* obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações (art. 189.º/2 do CPP)
   5.2. Pesquisa e apreensão de dados informáticos (arts. 15.º e 16.º da LCib)
   5.3. Apreensão de correio eletrónico e de registos de comunicações de natureza semelhante (art. 17.º da LCib) *vs.* apreensão de correspondência (art. 179.º CPP) *vs.* extensão do regime das intercepções telefónicas

(art. 189.º/1 do CPP)
5.4. Intercepção de comunicações (art. 18.º LCib)
5.5. Acções encobertas digitais (art. 19.º da LCib)
5.6. Monitorização on-line e falta de norma habilitante
5.7. Investigação criminal na *Dark Web*
5.8. Utilização de armadilhas digitais (malware)

6. Recolha de prova nas redes sociais

7. Cadeia de custódia e validade da prova

PARTE V – PRIVACIDADE *VS.* RECOLHA DE PROVA DIGITAL (ART. 8.º DA CEDH)

1. A jurisprudência do TEDH
2. As *Federal Guidelines for Searching and Seizing Computers*
3. A jurisprudência norte-*americana*
4. A *Plain View Doctrine* e a *Cyberplain View*

PARTE V – COOPERAÇÃO JUDICIÁRIA INTERNACIONAL

1. Crimes informáticos e aplicação da lei penal no espaço (artigo 27.º da LCib)
2. Acesso unilateral a dados armazenados em sistemas informáticos localizados no estrangeiro? (art. 15.º/5 e 25.º da LCib *vs.* arts. 31.º e 32.º, da Convenção sobre Cibercrime, e 24.º da LCib)
3. Âmbito da cooperação judiciária internacional (art. 20.º LCib)
4. O que veio trazer de novo o 2.º Protocolo Adicional relativo ao reforço da cooperação e da comunicação de provas eletrónicas (Estrasburgo, 28.05.2022)?

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

O programa está estruturado de maneira a proporcionar uma visão global da matéria do Cibercrime e da Prova Digital e a dar conta da sua complexidade teórica e relevância para a prática jurídica.
A escolha dos conteúdos programáticos pretendeu ir ao encontro dos conhecimentos, interesses e aptidões, tanto dos Alunos do Mestrado em Direito e Prática Jurídica, Especialidade de Direito Penal, como dos Alunos do Mestrado em Segurança da Informação e Direito no Ciberespaço, na sua esmagadora maioria sem formação jurídica.
O objectivo é impulsionar uma partilha de conhecimentos e uma aprendizagem conjunta, articulando a *expertise* técnica, dos Alunos do Mestrado em Segurança da Informação e Direito no Ciberespaço, quanto ao funcionamento dos sistemas informáticos, suas vulnerabilidades e recolha de prova em suporte electrónico, com o respectivo enquadramento jurídico no que concerne ao cibercrime e à prova digital. Isto no pressuposto de que o Direito Penal e Processual Penal não podem ser alheios à realidade do mundo digital, aos modos técnicos do seu funcionamento e do seu uso para a prática de crimes, nem à tecnologia necessária à recolha de prova digital e aos respectivos desafios técnico-jurídicos (*v.g.* cadeia de custódia e validade da prova, confronto com o direito à privacidade, conhecimentos fortuitos da investigação na busca digital).
Procura-se também ter em conta discussões contemporâneas quanto aos temas estruturantes do programa, quer nas aulas leccionadas pela Regente ou por especialistas convidados, quer nas exposições orais e nos trabalhos escritos apresentados pelos Alunos.
Tendo em conta a necessária diversidade da avaliação escrita dos Alunos do Mestrado em Direito e Prática Jurídica e dos Alunos do Mestrado em Segurança da Informação e Direito no Ciberespaço (dada a diferença da respectiva formação de base) e, ainda, o (escasso) número de aulas programadas (14), a Regente e os especialistas convidados leccionarão os temas estruturantes do programa, apresentando-se os demais conteúdos programáticos como uma lista de temas sugeridos aos alunos para as apresentações orais e os relatórios, destinados umas e outros ao aprofundamento e especificação de problemas relativos ao programa da UC de Cibercrime e Prova digital.
Nesta óptica, o programa servirá de ponto de referência comum às aulas ministradas pela Regente e por especialistas convidados e às escolhas dos temas e problemas concretos a tratar pelos Alunos nas exposições orais e nos relatórios, os quais nunca devem reflectir somente as suas opiniões baseadas em pré-compreensões sobre temas da cibercriminalidade e da prova digital, mas ter em conta o estado da arte e abrir-se às discussões contemporâneas do

problema escolhido como objecto da exposição oral e do relatório.

Metodologias de ensino (avaliação incluída)

I. O método

Tendo em conta o número de aulas previstas (14 de 100 minutos cada uma), estas seguem um modelo inicial de aulas teórico-práticas e depois de seminários científicos, com apresentação oral de trabalhos pelos mestrandos. Em qualquer um destes modelos, ocupam lugar de destaque: (i) a consideração de soluções legislativas portuguesas e estrangeiras (estas, designadamente em caso de ausência ou insuficiência da regulação nacional), e (ii) a análise crítica de jurisprudência nacional, estrangeira, do TEDH e do TJUE, referentes a questões jurídicas concretas.

As primeiras 10 aulas estão a cargo da Regente, incluindo a apresentação do programa e método de ensino (1 tempo lectivo) e preleções temáticas, algumas por especialistas convidados (advogados, magistrados e docentes universitários).

As restantes aulas (4) são dedicadas às apresentações de trabalhos pelos alunos, seguidas de discussão e debate por todos. Os temas e projectos das exposições orais e dos relatórios devem ser submetidos à aprovação prévia da Docente e obedecerão a um modelo comum (*Handout*). As exposições orais consistem na análise crítica de um ou mais acórdãos (portugueses, estrangeiros, do TEDH ou do TJUE) e de soluções legislativas nacionais e/ou estrangeiras a propósito de um concreto e bem delimitado problema jurídico do programa da UC. Realizar-se-ão 3 apresentações por aula, cada uma com a duração de 15-20 minutos, inultrapassáveis, seguidos de 10 minutos de debate.

II - Elementos de avaliação:

Segundo o n.º 1 artigo 30.º do Regulamento do Mestrado e do Doutoramento (https://www.fd.ulisboa.pt/wp-content/uploads/2023/05/Despacho-n.o-8673.2021-Alteracao-ao-Regulamento-do-Mestrado-e-do-Doutoramento-01.09.2021_compressed.pdf), a avaliação numa UC do Mestrado em Direito e Prática Jurídica compreende os seguintes elementos de aferição de conhecimentos:

a) Uma prova escrita obrigatória de avaliação final;

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 as aulas.

Na UC de Direito Penal V, é elemento de avaliação a apresentação voluntária de uma exposição oral sobre um tópico problemático do programa, seguida de discussão e debate por todos. São também considerados para efeitos da avaliação os projectos de exposição oral ou de relatório escrito, pré-submetidos à aprovação e orientação da regente, bem como a participação oral espontânea dos estudantes durante as aulas.

No caso dos Alunos do Mestrado em Segurança da Informação e Direito no Ciberespaço, por causa da diversidade da respectiva formação de base, o exame escrito final é substituído por um relatório sobre um concreto tópico problemático do programa, cujo tema e projecto deverão igualmente ser submetidos à aprovação e orientação da Regente. O relatório terá um *limite máximo inultrapassável de 10 páginas de texto* (excluindo, capa, índice, resumo e bibliografia), sendo o texto escrito em *Times New Roman, tamanho 12, espaço 1,5 no texto, e tamanho 10, 1 espaço nas notas de rodapé*. O Relatório deverá *seguir o template fornecido pela Regente e cumprir as regras do guião de citação de referências bibliográficas igualmente disponibilizado pela Docente*.

Dado o avultado número de alunos inscritos à disciplina (obrigatória na especialidade de Direito Penal do MDPJ), aos quais acrescem os Alunos do Mestrado em Segurança da Informação e Direito no Ciberespaço (24/26) e o número muito limitado de aulas (14), ambos inviabilizando a apresentação oral de trabalhos por todos os alunos e a avaliação contínua de tão grande número de alunos, *os discentes assíduos sem participação oral qualitativamente relevante terão, na parcela correspondente aos "Outros Elementos de Avaliação", a nota obtida no exame escrito final ou no relatório, para que a nota final não seja inferior à alcançada na prova escrita ou no relatório.*

Deste modo, não serão prejudicados os alunos assíduos, sem participação oral de relevo nas aulas, e os demais alunos sentir-se-ão incentivados a realizar a exposição oral de um trabalho e/ou a participar nas aulas, pois terão a possibilidade de ver recompensado o seu esforço para lá da mera assiduidade e da consideração da classificação obtida no exame escrito final ou no relatório para efeitos dos "Outros Elementos de Avaliação".

III - Assiduidade

Em cada aula realiza-se a chamada e regista-se as ausências dos Alunos. A falta a um número de aulas superior a um terço das previstas para a unidade curricular importa a perda de frequência e consequente reprovação na unidade curricular (artigo 13.º/1 e 2 do Regulamento). A falta da assiduidade mínima, tal como definida no artigo 13.º do Regulamento, impede também o acesso à época de recurso, uma vez que esta época tem por pressuposto a obtenção de nota negativa na unidade curricular (artigo 30.º/4 do Regulamento).

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

A aplicação do programa promove a constituição de um acervo que é acessível – designadamente através da criação de uma pasta colectiva na Dropbox – a todos os alunos da turma.
Nessa pasta serão disponibilizados: o programa da UC, com as metodologias de ensino e de avaliação, bem como a bibliografia básica; uma lista de bibliografia específica por temas; os textos-base, os PowerPoint ou os sumários referentes a cada aula; uma lista (indicativa) de possíveis temas para as exposições orais e os relatórios; um documento *word* (a preencher pelos alunos) com os temas-problemas escolhidos para as respectivas exposições e relatórios, os quais deverão seguir a ordem do programa da UC; elementos de apoio (legislação, doutrina e jurisprudência organizadas por temas); exames e testes (alguns resolvidos) de anos anteriores; o *Handout*, i.e., o modelo comum para apresentação do projecto de exposição oral ou do relatório; o calendário das exposições orais (a preencher pelos Alunos) as quais devem ter objectos-problema diversos e seguir a ordem dos conteúdos programáticos; um guião com regras de citação das fontes usadas nos relatórios; o formato-padrão (*template*) para o relatório.
Cada um dos Alunos deverá criar na pasta correspondente à sua turma e ao seu mestrado uma subpasta individual com o seu nome e número de aluno e nela depositará o respectivo *Handout* e depois o relatório, ambos serão directamente revistos e corrigidos na pasta da Dropbox pela Regente. Deste modo, existirá uma partilha de conhecimentos e da investigação realizada por cada Aluno, para que todos possamos aprender uns com os outros e, quanto às exposições orais, para que nas aulas a estas dedicadas cada aluno saiba o que nela vai ser discutido de modo a poder preparar-se para participar no debate.

Bibliografia Geral

I - PORTUGUESA

AA.VV.
(2018) *Cibercriminalidade e Prova Digital – Jurisdição Penal e Processual Penal* (Org.: CEJ), Lisboa: Coleção Formação Contínua (ebook).
(2020) *Cibercriminalidade e Prova Digital – Jurisdição Penal e Processual Penal. Atualização* (org.: CEJ), Lisboa: Coleção Formação Contínua (ebook).

AA.VV.
(2022) *Comentário Conimbricense do Código Penal. Parte Especial. Tomo II, Vol. I, Artigos 202.º a 254.º*, Coimbra: Gestlegal, 2.ª edição.

AA.VV.
(2019) *Comentário Judiciário do Código de Processo Penal*. Tomo II. Artigos 124.º a 190.º.

ALBUQUERQUE, Paulo Pinto de
(2022) *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos*, Lisboa: Universidade Católica Editora, 5.ª edição.

ALBUQUERQUE, Paulo Pinto de (Org.)
(2023) *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos*, Vol. I, Lisboa: Universidade Católica Editora, 5.ª edição.

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.

HENRIQUES GASPAR, António e outros
(2022) *Código de Processo Penal Comentado*, Coimbra: Almedina, 4.ª edição.

MACEDO, João Carlos Barbosa de

(2009) «Algumas considerações acerca dos crimes informáticos em Portugal», in AA.VV *Direito Penal hoje: Novos desafios e novas respostas* (org.: Manuel da Costa Andrade e Rita Castanheira Neves), Coimbra: Coimbra Editora, pp. 221-262.

MESQUITA, Paulo Dá,
(2010) «Prolegómenos sobre prova eletrónica e intercepção 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.

NUNES, Duarte Rodrigues
(2020) *Os crimes previstos na Lei do Cibercrime*, Coimbra: Gestlegal;
(2021) *Os meios de obtenção de prova previstos na Lei do Cibercrime,* 2.ª edição, Coimbra: Gestlegal;
(2024) *Os crimes previstos na Lei do Cibercrime e a responsabilidade penal dos entes colectivos. Atualizada à luz das Leis n.os 79/2021 e 94/2021*, Coimbra: Gestlegal, 2.ª edição (no prelo).

OLIVEIRA, Alexandre
(2021) «Prelúdios a uma revisitação da Lei do Cibercrime no âmbito da prova digital», in: AA.VV., *Corrupção em Portugal. Avaliação legislativa e propostas de reforma*, (org.: Paulo Pinto de Albuquerque, Rui Cardoso, Sónia Moura), Lisboa: Universidade Católica Editora, pp. 526-547.

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

VENÂNCIO, Pedro Dias,
(2011) *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora;
(2022) *Lições de Direito do Cibercrime e da tutela penal de dados pessoais*, Coimbra: Editora d'Ideias;
(2023) *Lei do Cibercrime – Anotada e Comentada. Atualizada pela lei nº 79/2821, de 24 de novembro*, Editora D'Ideias.

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 Ivridica* 320, pp. 717-749.

II – De Direito estrangeiro e comparado

ALMENAR PINEDA, Francisco
(2018) *Ciberdelincuencia. Teoría y práctica,* Porto: Juará Editorial.

CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo, e PAPA, Michele (Org.)
(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.

DELGADO MARTÍN, Joaquín
(2018) *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Madrid: La Ley/Wolters Kluwer España.

FERRER, Ezequiel (Dir.)
(2021) *Estudios de Cibercrimen*, Santiago-Chile: Editiones Olejnik.

HILGENDORF, Eric/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;
(2021) *Caselaw and Statutory Supplement to Computer Crime Law, 4th*, West Academic Publishing. Series: American Casebook Series.

LÓPEZ-MUÑOZ, Julián
(2020) *Cibercriminalidad e investigación tecnológica*, Madrid: Dykinson.

PINTO PALACIOS, Fernando/PUJOL CAPILLA
(2017) *La prueba en la era digital*, Madrid: La Ley/Wolters Kluwer España.

R. AGUSTINA, José/MIRÓ, Fernando (Dir.)
(2023) *Delitos* informáticos *y cibercriminalidad. Aspectos substantivos y procesales,* Montevideo/Buenos Aires: Editorial B de F.
REED, Chris,
(2011) *Computer Law*, 7.ª ed., Oxford: Oxford University Press.

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

ROMEO CASABONA, Carlos María/RUEDA MARTÍN, María Ángeles (Ed.)
(2023) *Derecho penal, ciberseguridad, ciberdelitos e Inteligencia Artificial*, *Volumen I: Ciberseguridad y ciberdelitos*, Granada: Comares.

SANZ DELGADO, Enrique/FERNÁNDEZ BERMEJO (Coord.)
(2021) *Tratado de delincuencia cibernética*, Navarra: Aranzadi.

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