CIBERCRIME: BREVE REFLEXÃO SOBRE CIBERINVESTIGAÇÃO EM TEMPO DE PANDEMIA

Ângelo Garcia Manuel Cambundo

Texto entregue em Novembro de 2021

O COMBATE AO CIBERCRIME CONSTA ENTRE OS OBJETIVOS definidos pela ONU na constituição e convenção da União Internacional de Telecomunicações, e é objeto da estratégia de segurança da União Europeia, mediante ação articulada da *European Network and Information Security Agency*, da *European Union Agenc y for Law Enforcement Cooperation*, do *European Cybercrime Centre* e da Agência Europeia de Defesa. Além disso, figura entre as preocupações permanentes da *The International Crime Police Organization*, que fornece apoio às polícias de investigação e autoridades judiciais. A título de bom exemplo, desde 2015 que Portugal possui uma estratégia nacional de segurança do ciberespaço (Resolução do Conselho de Ministros n.º 36/2015), que num de seus eixos prioriza o combate ao cibercrime. Para Elias (2018), o cibercrime é uma modalidade criminosa que aparece entre os principais riscos previstos na Lei das grandes operações do plano 2016-2019 e integra o rol dos objetivos prioritários da sua política criminal.

Conceito e caraterísticas

Para a Ciberinvestigação, apesar de eventuais lacunas legais, destacam-se os contributos da informática forense e a cooperação internacional nas sociedades contemporâneas pois, é permanente a tensão dialética entre a defesa das garantias e liberdades individuais do cidadão e a necessidade de imposição de restrições a essa autonomia em prol da segurança coletiva. Este debate, transcende o âmbito da Ciberinvestigação, constituindo, como afirmou James Q. Wilson, elemento essencial de qualquer sociedade livre (Kelling & Coles, 1997).

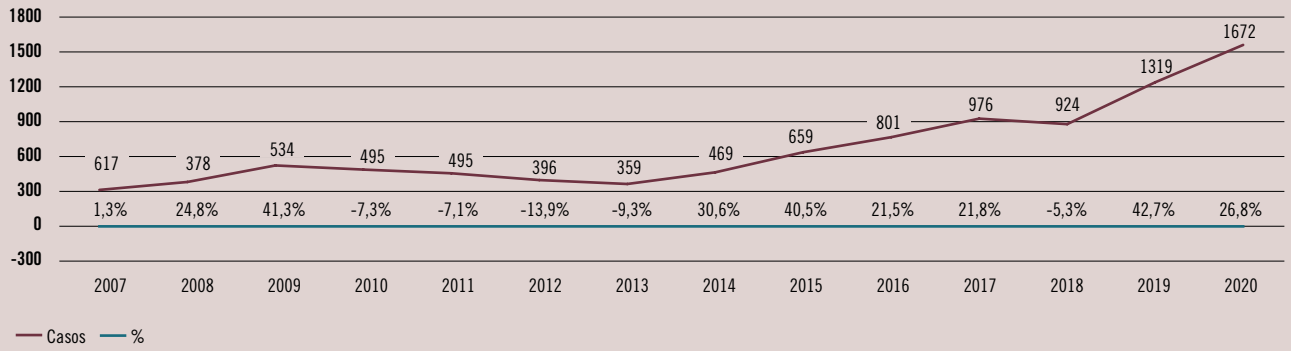
Para Costa & Melo (1999), entende-se como o ciberespaço, o espaço virtual de informação que se estabelece através da rede de computadores e telecomunicações. O cibercrime também designado por crime digital, crime informático, crime informático-digital, *high tecnology crime*, *computer-related crime* (Dias, 2012), não é de fácil conceituação, contudo, em 2007, a Comissão Europeia, tendo em vista uma política geral de luta contra este fenómeno definiu-o como um conjunto de atos criminosos praticados com recurso a redes de comunicações eletrónicas e sistemas de informação ou contra este tipo de redes e sistemas (Natário, 2013), ou seja, uma série de crimes praticados com recurso a novas tecnologias, como as de informação e de comunicação (Verdelho, Bravo, & Rocha, 2003). Por abranger novas modalidades criminosas e também crimes antigos praticados de formas novas, a Comissão Europeia divide o cibercrime em três categorias, nomeadamente os crimes tradicionais cometidos com o auxílio do computador e redes informáticas; os crimes relacionados com a publicação de conteúdos ilícitos por meios eletrónicos, e os crimes exclusivos das redes eletrónicas. A doutrina portuguesa distingue a criminalidade relacionada com a utilização de computadores em: crimes que recorrem a meios informáticos (a devassa por meio de informática e o crime de burla informática); crimes relativos à proteção de dados pessoais; crimes informáticos em sentido estrito (crimes praticados contra e através do computador também classificados como *vertical use of hi-tech*); e crimes relacionados com o conteúdo, onde se destacam a violação do direito de autor, a difusão de pornografia infantil, a discriminação racial ou religiosa (Dias, 2012). Dessa forma, a tipologia de cibercrimes mais recorrente compreende várias modalidades, designadamente, o *phishing* (criar página falsa de um banco, com o objetivo de adquirir dados financeiros ou números de cartões de crédito e senhas); o *carding* (a manipulação de elementos de identificação de cartões de crédito, de débito ou de telecomunicações); o *hacking* (a intrusão em sistemas informáticos); a pedofilia e a pirataria informática.

Em Portugal, não obstante a crise persistente socioeconómica e financeira a que se juntou a pandémica, tem-se registado um incremento da criminalidade informática participada, nomeadamente o acesso indevido ou ilegítimo, a falsidade informática, a reprodução ilegítima de programa protegido, a sabotagem informática, a viciação ou destruição de dados e outros crimes informáticos, representando um aumento de 353 casos (+26,8 %) de 2019 para 2020, numa análise desde 2007 sendo que, apenas no intervalo de 2010 a 2013 se registou um abrandamento significativo (Gráfico 1).

Natário (2013), algumas das características que costumam estar associadas ao cibercrime, são *a transnacionalidade* (a prática dos factos criminosos não implica a proximidade física entre o agressor e a vítima); *o anonimato* (os cibercriminosos conseguem facilmente utilizar identidades falsas, disseminar vírus, executar ataques e utilizar máquinas comprometidas por *malware* que permite o seu controlo remoto); *a tecnologia* (cujo avanço exponencial permite que se cometam milhares de crimes de forma rápida, sem esforço e com a garantia que a investigação a ser levada a cabo pelas autoridades competentes será difícil, desde logo pela complexidade na recolha da prova digital e pela existência de múltiplas ferramentas anti-forenses disponíveis aos criminosos); *a organização*, tendo em conta que muitos dos grupos criminosos são transnacionais e, geralmente, recrutam especialistas em informática para a prática de diversos crimes. A organização e o anonimato permitem aos cibercriminosos sobretudo o lucro fácil, operando de maneira concertada, a partir de pontos dispersos pelo mundo (Elias, 2018).

GRÁFICO 1 – INCREMENTO DA CRIMINALIDADE PARTICIPADA

Fonte: DGPJ



Evolução legislativa da Ciberinvestigação

A designada sociedade da informação surgiu como um campo de liberdade não regulado pelo Direito, contudo, a informática e sobretudo da internet trouxeram consigo novos instrumentos para a prática de crimes já conhecidos, e também, possibilitaram a prática de novas condutas carentes de tipificação penal. Tais, desafios foram ampliados pela dificuldade de fixar a competência territorial para persecução dos crimes e pela necessidade de harmonizar o dever de informar e o direito à privacidade, densificado na proteção dos dados pessoais. Em termos legais o marco é o Conselho da Europa de 2001, conhecida como a Convenção de Budapeste, que se consagrou como o instrumento internacional de maior importância na área do cibercrime, na medida que teve por fim proteger a sociedade do cibercrime, através da necessária adaptação legislativa e da melhoria da cooperação internacional. Ela, impôs aos Estados signatários a adequação do Direito Penal interno às especificidades destes crimes, visando a harmonização das legislações, sobretudo no âmbito do direito penal material e, assim, simplificar os processos de cooperação internacional (Dias, 2012). Portugal, somente em 2009, por meio da Resolução n.º 88/2009 da Assembleia da República e do Decreto Presidencial n.º 92/2009, ambos de 15 de setembro é que ratificou a Convenção de Budapeste, que havia assinado em 2001 e, na sequência, publicou a Lei n.º 109/2009 em 15 de setembro de 2009, a Lei sobre cibercrime, que revogou e substituiu a Lei 109/91, de 17 de agosto. Dessa forma, a Decisão-Quadro n.º 2005/222/JAJ do Conselho da Europa, de 24 de fevereiro foi transposta para a ordem jurídica interna, adaptando-se o direito interno à Convenção sobre Cibercrime do Conselho da Europa. A Convenção de Budapeste foi o primeiro trabalho internacional de grande relevo sobre o crime no ciberespaço, onde peritos e técnicos de todo o mundo participaram na sua elaboração, prevendo no seu artigo 12, que os Estados Membros estavam obrigados a tomar medidas de adequação da sua legislação interna à decisão-quadro até 16 de março de 2007, ou seja a Lei sobre Cibercrime surgiu, todavia, com dois anos de atraso.

Ciberinvestigação: possibilidades e dificuldades

A Lei do Cibercrime, nos termos de seu artigo 1.º, abarca não apenas as normas penais materiais e processuais, mas também as disposições inerentes à cooperação internacional em matéria penal, principalmente no que se refere à recolha de provas em suporte eletrónico, nomeadamente do *Internet Protocol*, no diálogo computacional, a localização dos dispositivos informáticos é realizada através de endereços de *Internet Protocol*, vulgarmente designados pelo acrónimo IP. Com efeito, é o IP que permite identificar um dispositivo numa miríade de máquinas que a todo o tempo estão conectadas à internet. Os IP podem ainda ser fixos ou dinâmicos. Nos fixos o mesmo IP está alocado a um determinado servidor e nos dinâmicos o IP varia de cada vez que o dispositivo se conecta com a rede. Os IP fixos são vulgarmente usados para identificar um servidor conectado com um determinado serviço que necessite de uma estabilização na respetiva identificação. É o que sucede com os *sites* de *internet*, que necessitam permanentemente da mesma identificação, pois, apenas dessa forma é possível aos dispositivos informáticos que a eles acedem reconhecerem a respetiva localização. Já o IP dinâmico são usualmente atribuídos pelos *Internet Service Providers* (ISP) aos respetivos clientes quando estes se conectam com a internet, fazendo parte do ativo empresarial dos ISP. Assim, cada vez que o cliente se liga à internet é-lhe atribuído um endereço IP explorado pelo ISP que providencia a ligação à internet.

> “O grande desafio que se apresenta à Ciberinvestigação é o de empregar métodos eficientes como os malwares e as ações encobertas, de forma ética, legal e moralmente legítima, visando à obtenção de provas reais num ambiente em permanente e vertiginosa evolução tecnológica.”

Em termos de investigação criminal, tal funcionamento significa que a identificação do cliente é realizada através dos seguintes passos: identificação do IP usado no acesso suspeito bem como o respetivo grupo data/hora; identificação do ISP possuidor do IP; solicitação ao ISP da identificação do cliente a quem foi atribuído o IP no identificado grupo data/hora. Esse sistema possui fragilidades, que podem fazer com que o cliente do IP identificado não seja o suspeito pela prática dos factos. Obviamente que o sistema se encontra dependente de identificar cada um dos clientes para o estabelecimento da ligação. Essa identificação é realizada com o conhecimento da porta de origem (conhecida pelo anglicismo *port*) do cliente individual em questão. Sucede, porém, que não é fácil identificar a porta de origem e, consequentemente, nem sempre é possível identificar o cliente suspeito. Para além disso, coloca-se o problema do respeito ao princípio da proporcionalidade e aos direitos, liberdades e garantias isto é, ao obter a lista de todos os clientes que usaram o referido IP, passa-se a possuir um conjunto de informações privadas de pessoas sem qualquer participação na prática dos factos ilícitos investigados. Ainda em matéria penal, no âmbito da recolha da Prova Digital, salientar que ela possui características como a efemeridade, fragilidade, volatilidade, imaterialidade, complexidade e codificação, dispersão, dinamismo e mutabilidade, universalidade, ubiquidade e transnacionalidade. Estas características tornam evidentes a dificuldade de obtenção e respetiva preservação, razão pela qual a Lei do Cibercrime teve o cuidado de tentar minimizar os efeitos nocivos desses obstáculos para a investigação criminal. Na dificuldade de definição legal de prova digital, devemos recorrer à construção doutrinária e jurisprudencial a fim de estabelecer um conceito, (Ramalho, 2017; Ramos, 2014). Nesta perspetiva, a prova digital é qualquer tipo de informação dotada de valor probatório, que esteja contida em dispositivo eletrónico ou que seja transmitida sob a forma binária ou digital através de sistemas e redes informáticas ou redes de comunicações eletrónicas, sejam elas privadas ou públicas (Rodrigues, 2011).

A lei do cibercrime foi criada em Budapeste em 23 de novembro de 2001, adotada em Portugal em 2009, e, é no contexto das dificuldades inerentes à produção da prova digital que surgem os art. 12.º a 19.º da Lei n.º 109/2009. A fim de bem compreender o seu alcance, convém referir o primeiro meio de produção da prova digital que é a preservação de dados informáticos. Refere ao regime da preservação expedita de dados, que diz respeito à emissão de uma ordem à pessoa ou entidade que possua a disponibilidade ou controlo de quaisquer dados informáticos específicos armazenados num sistema informático (Nunes, 2018). Segundo o autor, a preservação tem como objetivo manter os dados informáticos, bem como a respetiva integridade e confidencialidade, entendendo-se estes como os *dados de* identificação dos clientes, nomeadamente, nome, morada, contactos associados, IP estático, IP dinâmico unicamente nos casos em que esse IP for do conhecimento das autoridades e esteja em causa saber quem utilizou tal IP naquele momento, etc.; os *dados de tráfego* que são informações relativas às comunicações efetuadas pelos clientes onde se incluem as informações respeitantes ao IP dinâmico; os *dados de conteúdo* que concernem ao próprio teor da comunicação. A ordem de preservação de dados informáticos, deve referir a natureza dos factos a preservar, a sua origem, o seu destino, o período de tempo de preservação, que não pode ser superior a três meses, embora prorrogáveis até ao prazo máximo de um ano, sob pena de nulidade (Nunes, 2018).

Elencadas as características da prova digital, a investigação criminal depara-se com situações em que o destinatário da ordem de preservação dos dados não é o possuidor de todos os dados em causa, mas tem conhecimento de quem os possui. Assim, para obstar o comprometimento da investigação, a lei obriga o operador de comunicações a identificar tais entidades para que em relação a elas sejam emitidas as ordens de preservação de dados (Nunes, 2018). Segundo o autor, tendo em conta o art. 13º da Lei do Cibercrime, ante a inexistência de um catálogo de crimes restringindo sua incidência, o dispositivo é aplicável na investigação de qualquer espécie de delito, não se exigindo, de resto, que a medida surja como *ultima ratio*, pois dela se pode lançar mão sem necessidade de recorrer antes a outros métodos de colheita de prova. Após a identificação dos possuidores de informação probatória digital e da sua preservação, surge a necessidade de que ela seja obtida. Os dados informáticos podem ser de vários tipos, e sua natureza condiciona a forma como são recrutados para a investigação. Assim, no caso de dados base, a recolha é feita com base no disposto no artigo 14º da Lei do Cibercrime. A injunção prevista neste artigo é assim dirigida às pessoas ou entidades que possuam os dados base, sendo as mesmas obrigadas a fornecê-los sob pena de desobediência. Importa notar que tal obrigação deve ser entendida como benéfica para os possuidores das informações, pois a alternativa seria o recurso muito mais intrusivo e prejudicial para os direitos fundamentais, como as buscas e pesquisas informáticas feitas pelas autoridades, o que acarretaria mais custos pessoais e/ou humanos quer para os buscados quer para as autoridades de investigação criminal. Apesar disso, há na medida uma restrição aos direitos fundamentais, pois, como refere Nunes (2018), existe um acesso por parte das autoridades o que vai restringir a privacidade e a autodeterminação informacional, não existindo violação do direito à inviolabilidade das comunicações, precisamente porque a intrusão não é tão feroz como aquela que ocorre para a obtenção de dados de conteúdo ou de tráfego. Essa medida pode ser utilizada na investigação de qualquer crime, exigindo apenas que este meio seja necessário para a descoberta da verdade e que exista uma suspeita objetiva inicial. No que concerne à autoridade de que pode emanar tal ordem, a mesma varia conforme a fase do processo, ou seja, ao Ministério Público na fase de inquérito; ao Juiz de Instrução Criminal na fase de Instrução; ao Juiz na fase de julgamento. Quanto aos requisitos formais exige-se a identificação dos dados, embora a sua não referência consubstancia unicamente uma irregularidade que é sanável através da emissão de nova ordem (Nunes, 2018).

Ainda relativamente à produção da prova digital, o segundo meio é a Pesquisa de dados informáticos, que segundo o n.º1 do art.º 15.º, a pesquisa de dados informáticos é utilizada, quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático. A competência para autorizar ou ordenar este meio de obtenção de prova é da autoridade judiciária, nos termos do n.º1 do art.º 15.º, da Lei do Cibercrime. Entende-se por autoridade judiciária, nos termos do art.º 1.º, alínea b) do C.P.P o juiz, o juiz de instrução e o Ministério Público, cada um relativamente aos atos processuais que cabem na sua competência. Desse modo, a competência no que diz respeito a este meio de obtenção de prova "*é do magistrado do Ministério Público, na fase de inquérito, do juiz de instrução, na fase da instrução e do Juiz na fase de julgamento*" (Nunes, 2018:101). Tal norma deve ser interpretada no sentido de que a autorização para a realização desta diligência de investigação criminal tenha de ser judicial, nos termos do art.º 32.º n.º 4 da CRP (Rodrigues, 2011).

> "A cibercriminalidade, pelas suas características intrínsecas, apresenta às autoridades judiciárias dificuldades acrescidas no que concerne à identificação e a responsabilidade dos autores, bem como relativamente à recolha de prova digital."

Relativamente à apreensão de dados informáticos, convém referir que ela "*consiste em as autoridades obterem, para o processo, dados informáticos que se encontrem num sistema informático ou suporte autónomo que tenha sido alvo de uma pesquisa informática ou de outro acesso legítimo e que sejam necessários à descoberta da verdade material e/ou para a prova*" (Nunes, 2018, p. 117). Cumpre notar, aqui, que não raras vezes, no decurso de investigações, verifica-se a existência de informações livremente acessíveis e com relevância probatória em plataformas na internet (exemplo do Facebook). Quanto às ações encobertas em ambiente digital, a Lei do Cibercrime prevê no art.º 19.º o recurso às ações encobertas previstas na Lei 101/2001, de 25 de agosto, nos termos aí previstos e relativamente aos crimes elencados na alínea a) e b). A doutrina vem-se referindo a estas como ações encobertas em ambiente digital (Nunes, 2018), consubstanciando o reconhecimento da "*necessidade de recurso a métodos de investigação criminal mais agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis*" (Ramalho, 2013, pp.407-408).

O grande desafio que se apresenta à Ciberinvestigação é o de empregar métodos eficientes como os malwares e as ações encobertas, de forma ética, legal e moralmente legítima, visando à obtenção de provas reais num ambiente em permanente e vertiginosa evolução tecnológica. Deste modo, observa-se a velha máxima de que "*o processo penal é o direito constitucional aplicado, tem toda a razão de ser no campo da obtenção dos meios de prova*" (Mendes, 2018, pp.179).

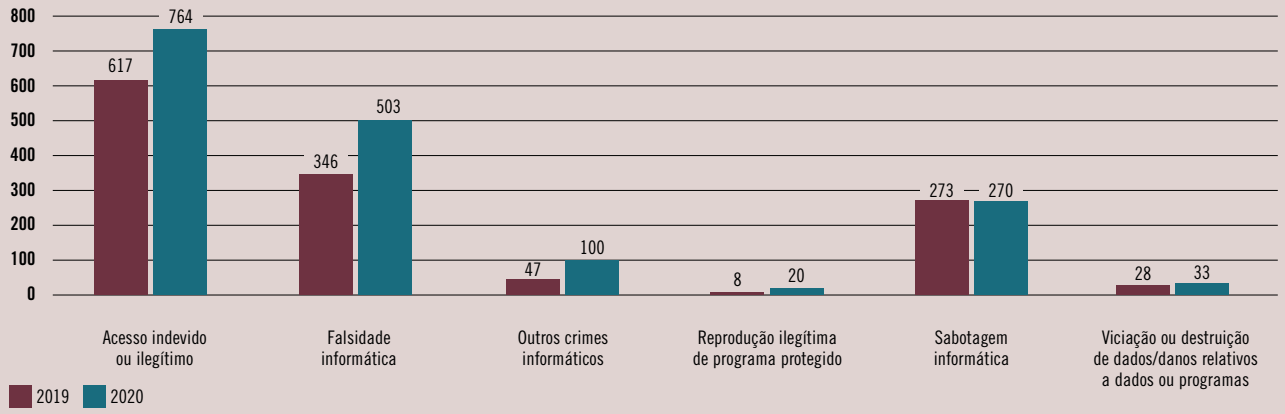
Cibercrime em tempos de crise pandémica

A cibercriminalidade pelas suas características intrínsecas, apresenta às autoridades judiciárias dificuldades acrescidas no que concerne à identificação e a responsabilidade dos autores, bem como relativamente à recolha de prova digital. Com efeito, basta imaginar um ataque contra uma infraestrutura crítica num determinado país a partir de qualquer parte do globo. Assim sendo, a cooperação internacional destaca-se como de fundamental importância, sobretudo no que tange a troca de informações e recolha de provas em suporte eletrónico. A Convenção de Budapeste, como anteriormente aflorado, teve como objetivo assegurar uma cooperação internacional entre os países, visando aproximar as nacionais e garantir uma resposta rápida e eficaz ao cibercrime transfronteiriço.

Através da Lei do Cibercrime, consagraram-se os instrumentos de cooperação internacional, que haviam sido previstos na Convenção do Cibercrime, tratada especificamente no capítulo IV. O artigo 20.º estabelece que as autoridades nacionais competentes cooperam com as autoridades estrangeiras para efeito de investigação e de recolha de provas em suporte eletrónico. Em Portugal, o artigo 21.º estabelece a Polícia Judiciária como ponto de contacto permanente para a cooperação internacional, assegurando a manutenção de uma estrutura que garanta um ponto de contacto disponível em permanência vinte e quatro horas por dia, durante os sete dias semanais. A grande evolução da nova lei ocorreu ao nível processual e da cooperação internacional, pois dentre as soluções apontadas para o combate a esta nova espécie de criminalidade, encontra-se a cooperação e coordenação internacionais de autoridades e entidades públicas e privadas (Dias,2012).

É de concordar com Dias (2012), quando salienta que somente com uma resposta global envolvendo uma governaça partilhada se poderá vencer a batalha contra o cibercrime transnacional, que, em contexto de crise pandémica, se apresenta como um crime dos

GRÁFICO 2 – TIPOLOGIA DA CRIMINALIDADE INFORMÁTICA PARTICIPADA
Fonte: DGPJ



novos tempos. Para reforçar a nossa breve reflexão sobre cibercrime, em Portugal, relativamente aos valores observados e respetivas variações de cada uma das tipologias que integram a criminalidade informática participada, os dados do relatório anual de segurança interna demonstram a gravidade deste tipo de crime (Gráfico 2).

Conclusão

Cremos ter conseguido a pretensão de apresentar sucintamente noções e conceitos básicos acerca do Cibercrime e a importância da cooperação internacional para o combate ao cibercrime.

Quanto às lacunas da Ciberinvestigação, nomeadamente no que se refere à utilização de meios e ações em ambiente digital que, observadas as peculiaridades do cibercrime, convém que se estabeleça uma tipologia dos métodos (de forma absoluta ou relativa) para sua investigação, de modo a balizar, com razoável segurança, os procedimentos para obtenção de provas. Para tal desígnio, sem prejuízo do suprimento das lacunas legais existentes, a investigação do cibercrime dependerá sempre do recurso a princípios como o da proporcionalidade e da ponderação de interesses, pois, a tensão entre a defesa das garantias e liberdades individuais do cidadão e a necessidade de imposição de restrições a essa autonomia em prol da segurança constitui circunstância permanente e inarredável da Ciberinvestigação. ■

Referências

Costa, J. & Melo, A. (1999). Dicionário Editora de Língua Portuguesa. 8ª Edição: Porto Editora

Dias, V. (2012). A Problemática da Investigação do Cibercrime. Data Vénia: *Revista Jurídica Digital*, Ano 1, N.º 1, julho – dezembro 2012

Elias, L. (2018). *Ciências policiais e segurança interna, desafios e prospetiva*. Instituto Superior de Ciências Policiais e Segurança Interna de Lisboa

Kelling, G.; Coles, C. (1997). *Fixing Broken Windows – restoring order and reducing crime in our communities*. Nova Iorque: Touchstone Book

Mendes, P. (2018). *Lições de Direito Processual Penal*. Almedina Editora.

Natário, R. (2013). O combate ao cibercrime: Anarquia e ordem no ciberespaço. Obtido em 15 de Março de 2018, de https://www.revistamilitar.pt/artigo/854

Ramalho, D. (2013). A investigação criminal na Dark Web. *Revista de Concorrência e Regulação*, Ano IV, n.º 14-15, pp. 383-429.

Ramalho, D. (2017). *Métodos ocultos de investigação criminal em ambiente digital*. Edições Almedina.

Ramos, A. (2014). *A prova digital em processo penal: O correio eletrónico*. Chiado Editora.

Ramos, A. (2015). A prova digital na investigação do (ciber) terrorismo. In *Investigação criminal n.º 9. Revista semestral de investigação criminal, ciências criminais e forenses* (pp. 110-134). Lisboa: ASFIC.

RASI.(2020). https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2021; acesso em 24 de novembro de 2021

Rodrigues, B. (2011). *Da prova penal tomo IV – Da prova eletrónico-digital e da criminalidade informático-digital*.

Verdelho, P., Bravo, R., & Rocha, M. (2003). *Leis do cibercrime* – Volume I. Edições Centro Atlântico