**Cenários/tópicos para o exercício sobre metodologia**

|  |
| --- |
| **Estudo de caso 1** Factos/cenário Bobby é polícia. Uma noite, está de serviço e vê um Mercedes estacionado à porta de sua casa. Não reconhece o automóvel, mas suspeita que este pertença ao chefe da sua mulher. Telefona para a esquadra e pede a Mary, a operadora informática, que lhe diga quem é proprietário do Mercedes, afirmando que o carro acabou de passar por um sinal vermelho. Mary confirma que o automóvel pertence efetivamente ao chefe da sua mulher.  *O Bobby cometeu uma infração penal?*   * **Problemas**   *O Bobby acedeu a um sistema informático? Esse acesso foi realizado de forma ilegítima?*   * **Pontos para discussão**   O computador foi acedido por Mary e não por Bobby e ela está autorizada a aceder aos dados do computador, sendo assim inocente. Foi Bobby quem, agindo através de uma agente inocente, provocou o acesso aos dados. Em conjunto com Mary (uma ilustração de engenharia social), isso corresponde a um acesso legítimo?  Tanto o Bobby como o Mary têm o direito de aceder ao computador da polícia, mas sujeitos a condições rigorosas relativas a uma consulta legítima no âmbito da atividade policial. Se o acesso ultrapassar esta autorização, tal constitui uma infração?  E se Bobby for à esquadra de polícia e conseguir olhar por cima do ombro de Mary (pirataria visual) enquanto ela está a efetuar uma pesquisa legítima sobre o proprietário do Mercedes?  A “pirataria visual” permitiu que Bobby tivesse acesso a dados informáticos. Pode colocar-se a questão da sua “intenção” e, evidentemente, ele não manipulou o sistema informático para obter acesso, mas ainda assim obteve acesso ilegítimo (embora tal seja muito difícil de provar).  Este estudo de caso destina-se a que os participantes considerem a questão da autorização (acesso ilegítimo).  Poder-se-ia igualmente solicitar aos participantes que avaliassem a situação em que Bobby entra na esquadra da polícia e consulta as informações sobre a propriedade do Mercedes num sistema de fichas de arquivo, sendo a informação idêntica à conservada no computador? A questão aqui é que não são apenas os dados em si que são protegidos (embora possam ser protegidos ao abrigo de outra legislação em matéria de proteção de dados, constituindo a má conduta de Bobby também uma infração), mas sim o suporte onde esses dados estão armazenados.  Os sistemas informáticos da polícia contêm grandes quantidades de informações pessoais relativas a indivíduos, em conjunto com muitas informações confidenciais. O acesso a esses dados só deve ser concedido às pessoas que tenham um interesse legítimo nos mesmos. No Reino Unido, verifica-se, com frequência, que os polícias e os informáticos da polícia acedem ilegalmente aos sistemas policiais para fins próprios, por exemplo, para encontrar informações que possam ter interesse para a imprensa ou, no caso de agentes corruptos, para descobrir quais as informações disponíveis sobre uma determinada pessoa ou se uma determinada pessoa ou grupo está ou não sob investigação ativa. |
| **Estudo de caso 2**   * **Factos/cenário**   Um segurança num banco é abordado por um grupo de criminosos que lhe pedem que coloque um dispositivo conhecido como *key logger* (registador de chaves) na parte posterior de vários terminais no banco. O *key logger* regista as teclas pressionadas pelo utilizador e obtém as palavras-passe e outras informações que permitiriam a alguém que teve acesso ao terminal aceder às contas de utilizador dos funcionários do banco.  Uma característica adicional do *key logger* permite-lhe gravar as chamadas telefónicas ou de Skype efetuadas pelo utilizador do terminal.  Os criminosos também colocaram uma escuta na secretária que capta som, incluindo todas as chamadas telefónicas realizadas e recebidas pelo utilizador do terminal.  *Houve interceção ilegal?*   * **Problema**   *Houve interceção?*  *Essa interceção foi conseguia por meios técnicos? Foram transmitidos dados de ou para um sistema informático?*   * **Pontos para discussão**   O *key logger* é um dispositivo técnico que capta dados transmitidos a partir do terminal. Isto equivale a uma interceção e é manifestamente ilegítimo.  E as chamadas de Skype? Neste cenário, afigura-se que os dados circulam na mesma linha que outros dados transmitidos a partir do computador, mas o que acontece se o utilizador tiver um telefone Skype autónomo? Esse telefone constituiria um sistema informático. A convenção define um “sistema informático” como *qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, realiza, em execução de um programa, o tratamento automatizado dos dados*; e “dados informáticos” como *qualquer representação de factos, de informações ou de conceitos sob uma forma suscetível de processamento num sistema informático, incluindo um programa, apto a fazer um sistema informático executar uma função*.  A utilização de uma escuta áudio pode ser um pouco mais difícil. Trata-se de uma “interceção”? No Reino Unido, os tribunais consideraram que, para que se verifique uma interceção, tem de haver algum tipo de interferência ou captação do sinal enquanto este estiver a ser transmitido na rede, neste caso a gravação tem lugar independentemente da transmissão, apesar de ser obtida a mesma informação caso o dispositivo tivesse sido colocado na “linha”.  E se o *key logger* tivesse sido colocado no sistema pela empresa que desejava garantir que os seus trabalhadores não utilizam a Internet para um fim inadequado?  A maioria dos sistemas de telecomunicações circula em redes públicas e privadas. No momento em que a comunicação deixa a sua propriedade, muda de um sistema privado para um sistema público. O responsável pelo tratamento de um sistema privado tem o direito de aceder às comunicações que utilizam esse sistema; assim, por exemplo, poderia monitorizar as conversas na sua linha telefónica doméstica, desde que qualquer dispositivo técnico que utilize para o efeito estivesse ligado ao lado privado do sistema.  Este cenário pretende que os participantes considerem cada um dos elementos da interceção e a existência de uma interceção de dados informáticos durante a sua transmissão por meios técnicos ilegítimos.  Deve ficar claro aos participantes que esta disposição se destina a proteger o conteúdo das comunicações e não as informações associadas ao endereçamento da mensagem ou o custo do serviço. |
| **Estudo de caso 3**   * **Factos/cenário**   Um grupo criminoso comunica através de um sistema de e-mail baseado na Internet que pode ser acedido através da Internet em qualquer parte do mundo. Em vez de enviarem mensagens entre si que possam ser intercetadas pela polícia ou que os possam incriminar se forem encontradas no seu computador, utilizam um sistema de “dead letter drop”. O que fazem é escrever a sua mensagem como um rascunho que nunca é enviado, os outros membros do grupo têm a palavra-passe que lhes permite aceder à conta de e-mail e ler e responder à mensagem.  Se a polícia pudesse aceder ao rascunho da caixa de e-mail, isso equivaleria a uma interceção?   * **Problemas**   *A mensagem é transmitida?*   * **Pontos para discussão**   A maioria dos Estados exige que a polícia estabeleça um elevado limiar de suspeita antes de autorizar a interceção do conteúdo de uma comunicação. A obtenção de provas sem a necessária autorização pode conduzir à suspensão do processo ou à inadmissibilidade das provas.  Os computadores e a Internet facilitam várias formas de comunicação, por exemplo, e-mail, mensagens instantâneas, Twitter, etc. As mensagens serão frequentemente armazenadas antes de serem recuperadas pelo destinatário previsto. Uma mensagem que ainda não foi recuperada deve ainda ser considerada como estando em curso de transmissão? Não é possível saber se o rascunho da mensagem foi lido pelo destinatário previsto. Deve a lei conceder a mesma proteção àqueles que optam deliberadamente por subverter os meios normais de envio de comunicações por e-mail à que dá a quem utiliza o e-mail da forma como foi concebido para ser utilizado?  Trata-se de uma forma bastante comum de os criminosos comunicarem entre si. A questão de procurar aceder a essas mensagens numa interceção ou não dependerá do direito interno ou da posição dos tribunais nacionais, mas pode ser útil que os participantes tenham consciência de que, se precisarem de recorrer a assistência jurídica mútua para obter esses dados, o Estado requerido pode considerá-la uma interceção ou, pelo menos, uma vez que o acesso ao conteúdo de uma comunicação está a ser solicitado, terá um limite legal superior que deve ser estabelecido para obter a autoridade judiciária necessária. |
| **Estudo de caso 4**   * **Factos/cenário**   O polícia Bobby levou o telefone da sua esposa, descobriu a sua palavra-passe e ouviu uma mensagem de voz armazenada que ela ainda não tinha recuperado.  *Trata-se de uma interceção?*   * **Problemas**   *A mensagem de voz está ainda em curso de transmissão? Houve interceção de dados informáticos?*   * **Pontos para discussão**   Até a mensagem chegar ao seu destino, está provavelmente ainda em curso de transmissão, apesar de estar armazenada no sistema. É provável que a mensagem esteja armazenada digitalmente no servidor da empresa telefónica, pelo que a Bobby acedeu a dados informáticos. O telefone é um computador? Provavelmente sim, uma vez que procede ao tratamento automatizado de dados. Os polícias que efetuam buscas e encontram telefones podem ter de considerar este aspeto para se certificarem de que dispõem da autoridade necessária para aceder a essas mensagens. Seria diferente se o destinatário tivesse ouvido a mensagem e optado por guardá-la.  Este cenário suscitou questões semelhantes às do cenário anterior. Serve para ilustrar o que pode ser uma situação bastante comum que pode aplicar-se igualmente aos polícias que executam um mandado de busca e apreendem um computador que contém tanto e-mails lidos como não lidos. Serve igualmente para ilustrar que a infração definida ao abrigo do Artigo 3.º se aplica a todas as formas de transferência eletrónica de dados, quer se trate de uma transferência por telefone, fax, e-mail ou ficheiro. |
| **Estudo de caso 5**   * **Factos/cenário**   Bobby interessa-se por OVNI e acredita que o governo russo capturou uma nave alienígena que aterrou na Sibéria no início do século XX. Visita um site de recrutamento militar russo que tem uma ligação a um site gerido pela Força Aérea russa. O site da Força Aérea requer uma palavra-passe, mas usando um dispositivo de decifragem de palavras-passe consegue obter acesso. Passa algum tempo a explorar o sistema e copia uma série de ficheiros. Tenta igualmente eliminar todos os ficheiros de registo da sua atividade para impedir que os russos o identifiquem. Em seguida, altera a página inicial do site de modo a que este apresente uma imagem de um OVNI em vez da insígnia da Força Aérea.  *O Bobby cometeu uma infração?* Problemas *O acesso não autorizado pode, por si só, constituir uma infração nos dados ou de interferência no sistema?*  *A supressão de provas de acesso não autorizado constitui uma infração?*  *É necessário provocar um prejuízo grave ao funcionamento do computador antes de poder ser alegada responsabilidade criminal?* Pontos para discussão As presentes disposições visam assegurar aos dados e programas informáticos uma proteção semelhante aquela de que gozam os bens corpóreos relativamente aos danos ocasionados de forma deliberada.  Bobby não estava autorizado a aceder ao site da Força Aérea, que estava protegido por palavra-passe. Por conseguinte, o acesso constitui uma infração de acesso ilícito.  Bobby suprimiu dados, os ficheiros de registo e a insígnia da Força Aérea. Embora talvez tenha sido ele a gerar os ficheiros de registo, estes não lhe pertencem e o sistema foi configurado para registar essa atividade. Não tem o direito de os apagar. A Força Aérea pode desejar saber quem tem acesso ao seu sistema.  Ao alterar a imagem na página inicial, suprimiu e adicionou dados ao sistema que, embora seja pouco provável que tenham resultado na perda de informações importantes, constituirá um embaraço para a Força Aérea. No entanto, mais importante ainda, embora Bobby possa alegar que apenas acedeu ao sistema para encontrar informações e que apenas apagou registos ou outros dados sem importância, pode qualquer administrador de sistemas ter confiança na integridade dos dados na sequência de tal intrusão ilícita?  A questão de saber se foi cometida uma infração nestas circunstâncias será uma questão de interpretação local. Pode acontecer que o limiar de gravidade não tenha sido estabelecido. No entanto, o administrador de sistemas sentir-se-ia provavelmente obrigado a colocar o site offline para determinar o efeito da intrusão, em particular se o site a que foi acedido contiver dados confidenciais ou sensíveis ou tiver sido utilizado em operações que, se viessem a correr mal, poria em perigo o público, como um sistema responsável pela gestão de uma central nuclear.  Se, para efeitos de argumentação, o sistema a que Bobby acedeu era o utilizado para gerir uma central nuclear, as infrações previstas nos Artigos 4.º e 5.º seriam adequadas para refletir a gravidade de tal intrusão, o que equivale a um ataque à infraestrutura crítica nacional? |
| **6. Estudo de caso 6** Factos/cenário Um programa automático de e-mail de *spam* envia diariamente e-mails não solicitados a milhares de utilizadores de todo o mundo. Se o e-mail for aberto, descarrega um software para a máquina do utilizador. O software não afeta o funcionamento do computador dos utilizadores, não obtém dados dos seus computadores, nem suprime quaisquer dados ou causa qualquer outro tipo de danos, mas faz com que o computador dos utilizadores seja agora um “zombie” que faz parte de uma “botnet” que o “controlador do bot” pode utilizar para realizar vários tipos de atividades.  *Foi cometida uma infração ao Artigo 4.º ou 5.º pela pessoa responsável pelo envio do spam?*   * **Problemas**   *Verificou-se algum acesso não autorizado à máquina do utilizador? Os dados foram alterados na máquina dos utilizadores?*  *Verificaram-se danos na máquina dos utilizadores?*   * **Pontos para discussão**   Embora não tenha sido causado qualquer dano, o software provoca uma alteração dos dados no computador dos utilizadores. Esta alteração não foi autorizada, uma vez que o utilizador não foi avisado nem convidado a dar o seu consentimento para a modificação do seu computador. O envio de *spam* é, por si só, ilegal ou é apenas um incómodo? Só se torna ilegal se tiver um impacto adverso?  E se o e-mail de *spam* contiver um anexo e um convite ao destinatário para abrir o anexo indicando “gostará disto”?  Poder-se-ia argumentar que o destinatário optou e, por conseguinte, consentiu em descarregar dados para o seu computador. No entanto, a realidade é que qualquer consentimento que possa ter sido dado não foi um consentimento informado, embora se possa argumentar que aqueles que optam por abrir anexos de remetentes desconhecidos o fazem por sua conta e risco.  Faz alguma diferença o facto de o utilizador não se importa que o seu computador passe ou não a fazer parte de uma “botnet”?  À medida que navegamos pela Internet, visitamos sites e descarregamos dados sem ter devidamente em conta a natureza do material que pode entrar no nosso computador, mas confiamos nos nomes que os sites lhes dão, nos nomes dos ficheiros ou nos resultados devolvidos pelo nosso motor de pesquisa para tomar as nossas decisões. Clicar numa imagem em miniatura para obter uma imagem de tamanho completo indica um conhecimento dos dados que pretendemos obter e um consentimento plenamente informado quanto à natureza desses dados. Se clicarmos numa imagem em miniatura de um automóvel apenas para verificar que a imagem em tamanho completo que obtemos é a de um avião, não se pode dizer que tenhamos dado o nosso consentimento para a obtenção desses dados.  A escolha de abrir uma ligação a um site resultará no descarregamento de muitos dados. Se o site for legítimo, a maior parte desses dados dirá provavelmente respeito ao conteúdo do site, embora uma parte possa consistir em anúncios publicados por terceiros. Mais uma vez, fizemos uma escolha informada e demos um consentimento implícito para receber o anúncio, sabendo que esta é uma prática comum na Internet. Uma prática comum no setor da Internet consiste em descarregar dados para o navegador dos utilizadores, os “cookies”.  Os cookies desempenham uma série de funções, incluindo o registo de um histórico de navegação na Internet. Será dada a um utilizador a opção de desativar a função de cookies no navegador; essa opção é suficiente para pressupor que o utilizador deu posteriormente o seu consentimento para o descarregamento desses dados? |
| **7. Estudo de caso 7**   * **Factos/cenário**   Bobby é um antigo polícia que foi demitido por utilização indevida do sistema informático da polícia. Decide vingar-se do departamento da polícia. Para o efeito, utiliza um programa de e-mail que lhe permite enviar 70.000 mensagens por hora para o seu antigo departamento. Altera o cabeçalho do e-mail para que pareça provir do chefe da polícia, enganando assim o servidor de e-mail da polícia para fazer crer que é proveniente de uma fonte legítima. O servidor da polícia não conseguiu gerir o volume de tráfego e entrou em colapso.  *Trata-se de uma infração de interferência do sistema?*   * **Problemas**   *O envio de um e-mail envolve o acesso ou a tentativa de acesso a um sistema informático, o servidor de e-mail*. *Em que medida é que o proprietário desse servidor autoriza esse acesso?*  *Se tiver um endereço de e-mail, tal não significa que está a convidar outros a enviarem-lhe mensagens de e-mail?*   * **Pontos para discussão**   Trata-se de uma questão de direito. O Bobby acedeu a um sistema e provocou o colapso do sistema através da introdução de dados. Ao criar um endereço de e-mail que é acessível ao público, o proprietário desse endereço dá implicitamente o seu consentimento à receção de mensagens. O Bobby pode alegar que a polícia deu o seu consentimento à receção de cada e-mail individual e que não é culpa sua que o sistema não tenha capacidade para lidar com tantas mensagens. Mas verificou-se realmente um consentimento? O proprietário de uma casa dá um consentimento implícito ao carteiro para entregar cartas que lhe são dirigidas na sua caixa de correio. Existe também um consentimento implícito para receber correio não solicitado, como os folhetos de pizzas. No entanto, o proprietário da casa não autoriza a receção de tantos folhetos de pizzas que não possa abrir a porta da frente.  Também é possível afirmar que, ao alterar os dados do remetente do e-mail, o acesso ao servidor de e-mail foi obtido através de fraude? A receção de tais e-mails enganosos (*spoofed*) não foi consentida.  Embora este cenário diga respeito a e-mails, o princípio aplica-se àqueles que procuram provocar o colapso de sites através de um ataque de negação de serviço, em que o site não consegue gerir o volume de tráfego que lhe é dirigido. A ligação a um site implica o intercâmbio de dados entre o computador dos utilizadores e o site. Também surgem questões semelhantes quanto ao consentimento implícito para a ligação ao site à semelhança do abordado em relação às mensagens de e-mail. |
| **Estudo de caso 8**   * **Factos/cenário**   Bobby envia um e-mail à sua mulher no seu local de trabalho. Altera o cabeçalho para fazer parecer que provém de uma das suas amigas. O e-mail contém um programa denominado “acesso a todas as áreas” que permite a Bobby assumir o controlo do computador da sua mulher. Antes de o Bobby ter a oportunidade de utilizar o programa, a sua presença é detetada pelo administrador do sistema, que fecha o sistema para proceder a uma avaliação da extensão da intrusão.  *O Bobby cometeu uma infração contemplada no Artigo 5.º?*   * **Problemas**   O Bobby provocou a supressão dos dados conservados no sistema? O Bobby prejudicou o funcionamento de um sistema informático?  Essa supressão de dados ou obstrução ao funcionamento do sistema foi ilícita?   * **Pontos para discussão**   A resposta do administrador do sistema ao e-mail do Bobby significa que o serviço foi negado aos utilizadores do sistema. Por conseguinte, o acesso aos dados conservados no sistema foi suprimido, embora seja provável que a restrição do acesso seja temporária. A infração não exige que os dados fiquem permanentemente indisponíveis.  Discutimos em que medida o proprietário de um endereço de e-mail autoriza a receção de dados de terceiros.  O Artigo 5.º diz respeito a sistemas informáticos, isto é, um ou mais computadores ligados entre si. Um computador isolado está ligado à parte da Internet de um sistema?  É muito provável que o computador de trabalho da mulher de Bobby faça parte de um sistema, mas faz provavelmente parte de uma LAN (Local Area Network) ou WAN (Wide Area Network) ou da Intranet. O Bobby prejudicou o funcionamento do sistema?  O Bobby poderá alegar que não é responsável pela negação de serviço e que não tinha intenção de provocar tal evento, pelo contrário, queria que o sistema continuasse a funcionar para que pudesse descobrir as intenções da sua mulher. Com frequência, os ataques de negação de serviço são insuficientes para colocar um site offline, mas os fornecedores de serviços colocarão o site offline para minimizar o efeito do ataque nos seus sistemas e reduzir os inconvenientes para outros clientes.  Neste cenário, não parece que Bobby tivesse a intenção para a prática de uma infração nos termos do Artigo 5.º, embora isso não signifique, evidentemente, que escape à sua responsabilidade criminal.  Este é um exemplo de um vírus de cavalo de Troia, que é uma forma comum de os criminosos informáticos acederem aos computadores de outros. |
| **9. Estudo de caso 9**   * **Factos/cenário**   Um grupo “hacktivista” online na Internet que protesta contra a utilização de animais para testar cosméticos realiza ataques de negação de serviço distribuído (DDOS) contra os sites de empresas de cosméticos e revistas de moda. Através do seu site, o grupo distribui o software que designa de “Supergun” que permite ao grupo coordenar ataques a sites e, assim, maximizar o volume de tráfego que pretende aceder a um site num determinado momento. O software “Supergun” foi originalmente desenvolvido como uma ferramenta pelos administradores de sistemas para testar a segurança dos seus sistemas. No entanto, embora o software continue a funcionar exatamente da mesma forma, a interface do utilizador foi tornada muito mais fácil de utilizar e apresenta agora o logótipo do grupo.  *A disponibilização do “Supergun” para descarregamento constitui uma infração? A posse do “Supergun” constitui uma infração?*   * **Problemas**   O facto de o “Supergun” poder ser utilizado para um fim legítimo significa que não é possível instaurar uma ação penal?  A disponibilização do “Supergun” para descarregamento é equivalente a distribuição?   * **Pontos para discussão**   As infrações a que se refere o presente artigo são: acesso não autorizado, interceção ilícita, interferência nos dados e no sistema.  Embora o software tenha originalmente uma dupla utilização, ou seja, uma função legítima, agora que a interface do utilizador foi alterada, isso significa que a sua posse, etc., constitui uma infração?  Olhando para os nossos estudos de casos anteriores, o software de “acesso a todas as áreas” utilizado por Bobby para aceder ao computador da sua mulher tem uma utilização legítima. Programas como este permitem que os utilizadores acedam remotamente aos seus próprios computadores. E relativamente à posse de Bobby de software de decifragem de palavras-passe, tratar-se-ia de uma infração? Pode tratar-se de uma questão de intenção, que razão legítima tem para possuir esse software? Existem provas que demonstrem que procurou utilizar este software para cometer uma infração?  Esta infração não se destina a ser utilizada para criminalizar os fornecedores e utilizadores legítimos de software. Quando, como aqui se verifica, existe prova de uma intenção dolosa, a questão talvez não se coloque. No entanto, as pessoas envolvidas no cibercrime também estão frequentemente envolvidas em atividades legítimas na Internet e podem muito bem ser profissionais do setor que utilizam e desenvolvem esse software, mas que, quando a oportunidade se apresenta, estão preparados para o aplicar na prossecução de atividades ilegais. E os lojistas? Como devem saber que intenção um cliente pode ter em relação a um determinado elemento de hardware ou de software. O âmbito da infração é demasiado vago? |
| **Estudo de caso 10**   * **Factos/cenário**   Um fornecedor de software produziu software de encriptação. O software divide o conteúdo do disco rígido em dois volumes, requerendo cada um deles uma palavra-passe para ter acesso, contudo somente um único volume estará disponível ao utilizador comum, não podendo a existência do volume oculto ser detetada através de software forense atualmente disponível.  O fabricante alega que este software seria útil para qualquer pessoa que se encontrasse numa situação em que está sob coação para revelar a sua palavra-passe. Tal significa que os dados no volume oculto podem ser mantidos seguros mesmo que a palavra-passe da pasta visível seja divulgada.   * **Problemas**   O fabrico, a produção, a distribuição, a utilização ou a posse deste tipo de software constitui uma infração penal?   * **Pontos para discussão**   Todos somos constantemente instados a manter os nossos dados seguros. Embora tal programa seja obviamente útil para os autores de crimes e, em especial, para aqueles que receiam que o conteúdo dos seus computadores os possa incriminar, não é por eles utilizado para cometer uma infração, mas sim para dissimular provas.  Os criminosos informáticos podem utilizar outros programas ou sistemas para evitar a deteção, incluindo anonimizadores, que lhes permitem navegar na Internet sem divulgar o seu verdadeiro endereço IP ou programas de eliminação de provas que podem apagar o conteúdo de um disco rígido. |
| **Estudo de caso 11**   * **Factos/cenário 3**   O Nick trabalha no departamento informático de uma grande empresa que tem a sua própria Intranet. A política da empresa proíbe os trabalhadores de utilizarem o seu computador e a respetiva ligação à Internet para efetuarem compras online. No seu tempo livre, Nick começa a desenvolver um software que permitiria à empresa identificar os trabalhadores que efetuam pagamentos online e recolher essas informações para que possam ser utilizadas como prova em processos disciplinares. Nick não possui as competências necessárias e entra em contacto online com “Jupiter”. Em conjunto, desenvolvem um software que, uma vez descarregado para o computador de um utilizador se ativa quando esse utilizador começar a preencher um formulário online, como os utilizados para processar pagamentos online, e captará os dados introduzidos pelo utilizador. A empresa da Nick está muito satisfeita, ao passo que Jupiter começa a distribuir o software utilizando um programa de cavalo de Troia.  *O Nick cometeu uma infração?*  *A empresa cometeu uma infração? O Jupiter cometeu uma infração?*   * **Problemas**   O dispositivo foi concebido ou adaptado principalmente com o objetivo de cometer as infrações penais indicadas?   * **Pontos para discussão**   Os criminosos informáticos podem aceder a uma variedade de ferramentas que lhes permitem cometer infrações ou que os ajudarão a fazê-lo. É possível adquirir o código que lhe permitirá construir o seu próprio “bot” ou adquirir uma “botnet” ou o acesso a uma “botnet” que possibilite ao utilizador cometer vários tipos de crime, como o “phishing”.  O Jupiter utilizará este programa para obter dados financeiros dos utilizadores que podem ser explorados pelo próprio Jupiter ou por outros. A empresa presumivelmente pensou que Nick o tinha produzido no âmbito do seu trabalho. Nick é inocente e ajudou inadvertidamente Jupiter a criar uma poderosa ferramenta criminosa. Nem Nick nem a empresa apresentam a intenção criminosa exigida. Seria diferente se o Jupiter comercializasse o programa a outras empresas que pretendessem controlar a atividade dos seus trabalhadores na Internet? Pode o Jupiter argumentar que o software tem um objetivo legítimo, apesar da sua óbvia atração para criminosos? |
| **Estudo de caso 12**   * **Factos/cenário**   Stefan utiliza um software fotográfico comercialmente disponível para produzir uma carta de crédito realista no seu computador doméstico. Leva a carta de crédito ao seu banco, que a aceita como autêntica e transfere fundos para a conta de Stefan.  *Que infração cometeu Stefan?*   * **Problemas**   A produção de cartas de crédito falsificadas é considerada falsidade informática?  A infração só é considerada cumprida depois de o funcionário do banco aceitar a carta de crédito falsificada como autêntica?   * **Pontos para discussão**   A criação de uma carta de crédito envolve a introdução de dados não autênticos num computador, ou seja, que a carta de crédito tenha sido elaborada a favor de Stefan.  No entanto, tal foi realizado de forma ilícita ou Stefan tem o direito de apresentar esse documento no seu próprio computador? Stefan pode ter a intenção de utilizar a carta de crédito para defraudar o banco, mas, por qualquer motivo, pode nunca imprimir a carta. É relevante para a responsabilidade de Stefan o facto de o documento nunca ser apresentado em papel?  Esta infração não foi, na verdade, criada para lidar com este tipo de cenário, embora possa servir se a legislação nacional não criminalizar, de outro modo, a produção de uma carta de crédito falsificada. Estas infrações podem ser antes consideradas em termos de responsabilidade subsidiária, como a tentativa.  Esta infração destina-se, na realidade, a quem utiliza um computador como mecanismo para cometer a infração, ou seja, quando age de boa-fé, o funcionário bancário introduz os dados fornecidos por Stefan, aceitando que os dados são autênticos. |
| **Estudo de caso 13**   * **Factos/cenário**   Stefan sempre se gabou perante os seus amigos das suas proezas como atleta quando era adolescente. Os seus amigos são céticos. Consegue aceder à base de dados da sua antiga escola e altera os registos para o mostrar como capitão do grupo de atletismo da escola e mostrar que conquistou várias medalhas.  *Trata-se de um crime de falsidade informática?*   * **Problema**   Os dados alterados não serão utilizados para qualquer efeito legal.   * **Pontos para discussão**   Stefan alterou os dados e introduziu dados falsos. É evidente que este acesso e alteração são ilícitos. Independentemente das outras infrações que Stefan possa ter cometido, é duvidoso que tenha cometido falsidade informática, uma vez que estes dados não serão utilizados para efeitos legais.  A infração relacionada com a falsificação não diz respeito a ganhos financeiros ou outros; estas infrações inscrevem-se no âmbito de burla informática. Este artigo visa assegurar a segurança e credibilidade dos dados eletrónicos que poderão ter consequências ao nível das relações jurídicas. A expressão “para fins legais” refere-se igualmente às transações e aos documentos que são relevantes nos termos da lei. |
| **Estudo de caso 14**   * **Factos/cenário**   Agora que perdeu o seu emprego na polícia e tem de pagar uma pensão de alimentos à sua mulher desde o divórcio, Bobby está à procura de outra forma de ganhar dinheiro. Sempre se interessou por ações e adquire 1000 ações da Flanders Mining Inc., uma sociedade com direito exclusivo de extração de urânio na Bélgica por 1 euro cada. O Bobby é membro de um fórum na Internet cujos membros estão, como o Bobby, interessados no mercado bolsista. Bobby envia uma mensagem em que afirma que um amigo do governo belga lhe disse que tinham sido detetadas quantidades substanciais de urânio na Bélgica. Na sequência deste anúncio, o preço das ações da Flanders Mining Inc. dispara e no fim da semana, cada ação vale 1000 euros. Nessa altura, o Bobby vende as suas ações.  *O Bobby cometeu uma infração?*   * **Problemas**   A mensagem de Bobby não é verdadeira?  Se a mensagem não era verdadeira, outra pessoa perdeu bens devido a isso? O Bobby obteve uma vantagem económica?   * **Pontos para discussão**   Se a mensagem enviada por Bobby não for verdadeira, então poderá ter cometido uma infração. Introduziu dados falsos num computador e obteve benefício económico para si próprio com o aumento do preço das ações.  A relação causal entre a introdução dos dados e o efeito é muito distante?  O Bobby prejudicou outros? Provavelmente sim, na medida em que as ações são incorretamente avaliadas e, em algum momento, o seu preço iria presumivelmente diminuir. No entanto, é de reconhecer que o mercado de ações é extremamente volátil, sendo que o valor de uma ação é o preço que uma pessoa está disposta a pagar por ela num determinado momento.  Alguém foi realmente defraudado? Estes tipos de rumores e mensagens não são abundantes na Internet? Alguém vai realmente acreditar nesta publicação ou não a encarar como uma tentativa “atrapalhada” de manipular o preço das ações? Significa isto que não podemos mentir na Internet? |
| **Estudo de caso 15**   * **Factos/cenário**   Stefan dirige-se ao banco. No parque de estacionamento verifica que não tem moedas pequenas. Coloca uma arruela na máquina de estacionamento automática e obtém um bilhete.  *Stefan cometeu uma infração?*   * **Problemas**   A máquina de estacionamento é um computador?  É importante o facto de a máquina de estacionamento emitir automaticamente bilhetes e de nenhum ser humano ter sido enganado?  Qual é o estatuto do bilhete de estacionamento?   * **Pontos para discussão**   A máquina de estacionamento é um computador que processa os dados, que calcula o montante do dinheiro em função da tarifa de estacionamento e emite um bilhete durante o período de tempo apropriado. Stefan introduziu dados inautênticos, uma arruela e não uma moeda adequada. O Artigo 7.º não exige que um ser humano tenha agido com base nos dados fornecidos.  O bilhete de estacionamento é uma falsificação, os dados utilizados para o criar eram falsos e foi produzido para que uma pessoa, o funcionário do estacionamento, o considerasse genuíno e não passasse a Stefan uma multa de estacionamento. |
| **Estudo de caso 16**   * **Factos/cenário**   Após a sua detenção, a polícia descobre que Stefan está na posse de dados de cartões de crédito pertencentes a um grande número de terceiros.  *A posse destes dados constitui uma infração penal?*   * **Problemas**   Qual o estatuto dos ficheiros informáticos? São considerados “bens” em termos de direito, apesar do facto de todos serem constituídos por uma cadeia de código binário?   * **Pontos para discussão**   No Reino Unido, a posse de um artigo para fins fraudulentos constitui uma infração penal substantiva. O artigo inclui um ficheiro informático. É claro que é necessário provar a respetiva intenção, mas é difícil argumentar um motivo legítimo para estar na posse de dados deste tipo.  Pode acontecer que se considere que se trata de uma infração preparatória. |
| **Estudo de caso 17**   * **Factos/cenário**   Adam é membro de um grupo exclusivo online que realiza o intercâmbio de fotografias de crianças a serem vítimas de abusos sexuais. Adam é também membro de um grupo de partilha de ficheiros “entre pares”, publica fotografias de crianças a serem vítimas de abuso que obteve do grupo online em pastas partilhadas entre pares, o que as torna acessíveis a outras pessoas na rede de pares.  *Quais as infrações cometidas por Adam?*   * **Problemas**   Definições de produção, obtenção e distribuição.  Adam descarregou ficheiros de imagens da Internet. O descarregamento equivale à produção de tal imagem? Descarregar e, em especial, guardar uma imagem num computador não é igual a ver televisão. O ato de descarregar cria algo novo, um ficheiro informático que permite visualizar imagens na Internet, o que implica a produção de novas imagens. Este conceito pode ser útil para os procuradores.  As redes de partilha de ficheiros entre pares permitem aos membros aceder aos ficheiros que lhes são disponibilizados por outros membros da rede. Ao colocar as imagens na pasta comum, Adam está a disponibilizá-las para distribuição. |
| **Estudo de caso 18**   * **Factos/cenário**   Bill é detido no aeroporto quando regressa do Camboja. O seu computador portátil contém um grande número de imagens do seu envolvimento em atividades sexuais com crianças que parecem ser do Sudeste Asiático.  *Pode Bill ser processado em relação às imagens?*   * **Problemas**   Competência.  Escolha da infração substantiva, estar posse de uma imagem ou realização da mesma.   * **Pontos para discussão**   Podem existir questões jurisdicionais relacionadas com a produção das imagens, uma vez que parecem ter sido produzidas no estrangeiro.  A posse não deve constituir um problema. |
| **Estudo de caso 19**   * **Factos/cenário**   [WWW.Iuvfishin.com](http://WWW.Iuvfishin.com/) é um site dedicado à pesca. O site está alojado em servidores localizados nos EUA. Os proprietários do site descobrem que foi pirateado e que foram carregadas e integradas no site milhares de imagens de abusos de crianças. A forma como tal foi realizado significa que estas imagens não seriam visíveis aos utilizadores comuns do site. O site regista os endereços IP das pessoas que acederam às fotografias.  Um endereço IP atribuído a John foi dado à polícia do seu país. Esta procura o endereço de John e apreende o seu computador, que contém milhares de imagens de abusos de crianças. Do historial na Internet e dos dados contidos nestes ficheiros fica claro que a maioria das imagens foi descarregada da Internet.   * **Problemas**   Como provar que John é responsável pelas imagens? O impacto para os suspeitos acusados de crimes de pedofilia.   * **Pontos para discussão**   Este método de dissimular imagens não é invulgar. Os grupos publicarão ligações às imagens. No entanto, poderá ser perigoso confiar apenas no endereço IP para obter um mandado de busca sem compreender a forma como esse endereço IP foi registado no site, podendo ter sido encaminhado de forma totalmente inofensiva por outro site e não ter acedido a quaisquer imagens depois de se ter apercebido do que eram. Obviamente, podem ter visitado o site mais do que uma vez ou ter acedido a várias imagens.  Pode utilizar isto para discutir os cuidados necessários antes de acusar um indivíduo de ser um pedófilo. Existe uma elevada taxa de suicídio entre as pessoas acusadas destes crimes. Como em todos os casos de cibercrime é necessário conseguir colocar o suspeito no teclado no momento relevante, um endereço IP pode ser utilizado por várias pessoas no mesmo endereço ou a rede sem fios pode ter sido pirateada por outra pessoa. As acusações deste tipo podem ter um efeito devastador sobre um indivíduo inocente. |
| **Estudo de caso 20**   * **Factos/cenário**   A polícia dos EUA retirou um site que aloja sites que disponibilizam imagens de abusos de crianças a quem pagar uma assinatura mensal. As autoridades dos EUA recolheram dados daqueles que pagaram pelo acesso, incluindo o endereço IP, os números do cartão de crédito, o endereço de e-mail, o endereço de faturação e a palavra-passe. Um dos clientes é Oswald. Após ter obtido um mandado de busca, o seu computador é examinado. Não se encontra nada incriminatório porque Oswald utilizou um programa denominado “Eliminação de provas”.  *O Oswald cometeu uma infração?*   * **Problemas**   O Oswald cometeu uma infração substantiva ou uma responsabilidade subsidiária? Existem questões relacionadas com a competência?  É importante que o site dos EUA tenha sido totalmente automatizado?  O que afirmamos sobre a utilização do programa de eliminação de provas?   * **Pontos para discussão**   Oswald não está na posse de quaisquer imagens e não podemos provar que tenha alguma vez acedido a um site para visualizar essas imagens, embora possamos provar que pagou uma assinatura para o fazer. No entanto, Oswald pagou dinheiro para persuadir outra pessoa, o proprietário do site nos EUA a distribuir ou a disponibilizar imagens de abusos de crianças para distribuição. Trata-se, portanto, de uma infração?  O facto de o site nos EUA ser totalmente automatizado, significa que nenhum ser humano está efetivamente envolvido no tratamento dos dados dos cartões de crédito. Mesmo assim, o processo foi criado e é administrado e mantido por uma pessoa que beneficia financeiramente.  A utilização de um programa de eliminação de provas não é, por si só, ilegal. A menos que Oswald tenha sido capaz de ativar o programa durante a investigação policial, é pouco provável que tenha cometido uma infração relacionada com a administração da justiça.  No entanto, se Oswald for processado, a utilização desses programas pode ser considerada como um elemento agravante pelo tribunal. |