**Escenarios/temas para el ejercicio metodológico**

|  |
| --- |
| **Estudio de caso 1** Hechos / escenario Bobby es un agente de policía. Una noche está de servicio y ve un Mercedes aparcado frente a su casa. No reconoce el coche, pero sospecha que pertenece al jefe de su mujer. Llama por teléfono a la comisaría y pide a Mary, la operadora informática, que le diga de quién es el Mercedes, diciendo que el coche acaba de saltarse un semáforo en rojo. Mary le confirma que el coche pertenece efectivamente al jefe de su mujer.  *¿Ha cometido Bobby un delito?*   * **Preguntas**   *¿Ha accedido Bobby a un sistema informático? ¿Fue un acceso ilegítimo?*   * **Puntos de debate**   María accedió al ordenador, no Bobby. Ella está autorizada a acceder a los datos del ordenador, es inocente. Fue Bobby quien, actuando a través de un agente inocente, provocó el acceso a los datos. Le mintió a María (un ejemplo de ingeniería social), ¿esto equivale a un acceso en derecho?  Tanto Bobby como Mary tienen derecho a acceder al ordenador de la Policía, pero bajo estrictas condiciones relacionadas con una consulta legítima en relación con la actividad policial. Si el acceso excede esta autorización, ¿constituye esto un delito?  ¿Qué ocurre si Bobby fuera a la comisaría y consiguiera mirar por encima del hombro de Mary (shoulder surfing) mientras ella está haciendo una consulta legítima en relación con la propiedad del Mercedes?  El "shoulder surfing" ha permito que Bobby acceda a datos informáticos. Puede que se cuestione su "intención" y, por supuesto, no ha manipulado el sistema informático para obtener el acceso, pero ha obtenido el acceso de manera ilegítima (aunque esto sería muy difícil de demostrar).  Este estudio de caso está diseñado para que los delegados consideren la cuestión de la autorización (acceso de manera ilegítima).  También se puede pedir a los participantes que consideren la situación si Bobby hubiera ido a la comisaría y hubiera buscado la información sobre la propiedad del Mercedes en un sistema de fichas, ya que la información es la misma que se guarda en el ordenador. La cuestión aquí es que no son los datos en sí los que están protegidos (aunque pueden estarlo en virtud de otra legislación de protección de datos, mientras que la conducta indebida de Bobby también podría constituir un delito), sino que es el medio en el que se almacenan los datos el que está protegido.  Los sistemas informáticos de la Policía contienen grandes cantidades de información personal relacionada con los individuos, junto con mucha información sensible. El acceso a estos datos solo debe concederse a quienes tengan un interés legítimo en ellos. En el Reino Unido es frecuente que los agentes de policía y los operadores informáticos de la Policía accedan ilegalmente a los sistemas policiales con fines propios, por ejemplo, para encontrar información que pueda interesar a la prensa o, en el caso de los agentes corruptos, para descubrir qué información se tiene sobre una persona concreta o si una persona o un grupo concreto están siendo investigados. |
| **Estudio de caso 2**   * **Hechos / escenario**   Un guardia de seguridad de un banco es abordado por un grupo de delincuentes que le piden que coloque un dispositivo conocido como key logger (registrador de teclas) en la parte posterior de varios terminales del banco. El registrador de teclas registra las pulsaciones del usuario y captura las contraseñas y otra información que permitiría a alguien que tuviera acceso al terminal entrar en las cuentas de usuario del personal del banco.  Una característica adicional del registrador de teclas le permitía grabar las llamadas telefónicas de Skype realizadas por el usuario del terminal.  Los delincuentes también colocaron un micrófono en el escritorio que captaba el sonido, en particular todas las llamadas telefónicas realizadas y recibidas por el usuario del terminal.  *¿Se ha producido una interceptación ilícita?*   * **Preguntas**   *¿Se ha producido una interceptación?*  *¿Se ha logrado esa interceptación por medios técnicos? ¿Se han transmitido datos hacia o desde un sistema informático?*   * **Puntos de debate**   El registrador de teclas es un dispositivo técnico que capta los datos que se transmite desde el terminal. Esto equivale a una interceptación y está claramente fuera de lugar.  ¿Qué pasa con las llamadas de Skype? En este caso, parece que los datos viajan por la misma línea que otros datos transmitidos desde el ordenador, pero ¿qué pasa si el usuario tiene un teléfono Skype independiente? ¿Constituiría dicho teléfono un sistema informático? El Convenio define un "sistema informático" como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa; y "datos informáticos" como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.  El uso del micrófono de audio puede ser un poco más difícil. ¿Se trata de una "interceptación"? En el Reino Unido, los tribunales han sostenido que, para que se produzca una interceptación, tiene que haber algún tipo de interferencia o abstracción de la señal mientras se transmite por la red; en este caso, la grabación tiene lugar independientemente de la transmisión, aunque se obtenga la misma información si el dispositivo se hubiera colocado en la "línea".  ¿Qué ocurre si el registrador de teclas fue colocado en el sistema por la empresa, que está preocupada por asegurar que sus empleados no utilizan Internet con fines inapropiados?  La mayoría de los sistemas de telecomunicaciones viajan por redes públicas y privadas. En el momento en que la comunicación sale de su propiedad, pasa de un sistema privado a un sistema público. El controlador de un sistema privado tiene derecho a acceder a las comunicaciones que utilizan ese sistema; así, por ejemplo, podría vigilar las conversaciones en la línea telefónica de su casa siempre que el dispositivo técnico que utilice para ello esté conectado a la parte privada del sistema.  Este escenario está diseñado para que los delegados consideren cada uno de los elementos de la interceptación, es decir, que haya una interceptación de datos informáticos en el curso de su transmisión por medios técnicos de manera ilegítima.  Los delegados deben tener claro que esta disposición está diseñada para proteger el contenido de las comunicaciones y no la información relacionada con el direccionamiento del mensaje o el coste del servicio. |
| **Estudio de caso 3**   * **Hechos / escenario**   Una banda de delincuentes se comunica utilizando un sistema de correo electrónico basado en la web al que se puede acceder a través de Internet en cualquier parte del mundo. En lugar de enviarse mensajes que puedan ser interceptados por la Policía o que puedan incriminarles si se encuentran en su ordenador, utilizan un sistema de "carta muerta". Lo que hacen es escribir su mensaje como un borrador que nunca se envía, otros miembros de la banda tienen la contraseña que les permite acceder a la cuenta de correo electrónico y leer y responder al mensaje.  Si la Policía pudiera acceder al borrador del buzón de correo electrónico, ¿se trataría de una interceptación?   * **Preguntas**   *¿Se está transmitiendo el mensaje?*   * **Puntos de debate**   La mayoría de los Estados exigen que la Policía establezca un alto umbral de sospecha antes de autorizar la interceptación del contenido de una comunicación. La obtención de pruebas sin la autorización necesaria puede dar lugar a la paralización del caso o a la inadmisibilidad de las pruebas.  Los ordenadores e Internet facilitan diversas formas de comunicación, como el correo electrónico, la mensajería instantánea, Twitter, etc. Con frecuencia, los mensajes se almacenan antes de ser recuperados por el destinatario. ¿Debe considerarse que un mensaje que aún no ha sido recuperado está en curso de transmisión? No hay forma de saber si el borrador del mensaje ha sido leído por el destinatario. ¿Debe la ley conceder la misma protección a quienes deliberadamente deciden subvertir los medios normales de envío de comunicaciones por correo electrónico que la que concede a quienes utilizan el correo electrónico tal como fue concebido?  Esta es una forma bastante común de comunicación entre los delincuentes. El hecho de que se intente acceder a estos mensajes en una interceptación o no dependerá de la legislación nacional y/o de la actitud de los tribunales nacionales, pero puede ser conveniente que los delegados se den cuenta de que si necesitan recurrir a la asistencia judicial recíproca para obtener estos datos, el Estado requerido puede considerarlo una interceptación o, al menos, debido a que se busca el acceso al contenido de una comunicación, tendrá un umbral legal más alto que debe establecerse para obtener la autoridad judicial necesaria. |
| **Estudio de caso 4**   * **Hechos / escenario**   El agente de policía Bobby ha cogido el teléfono de su mujer, ha adivinado su contraseña y ha escuchado un mensaje de voz almacenado que ella aún no ha recuperado.  *¿Se trata de una interceptación?*   * **Preguntas**   *¿Está el mensaje de voz todavía en curso de transmisión? ¿Se ha producido una interceptación de datos informáticos?*   * **Puntos de debate**   Hasta que el mensaje no haya llegado a su destino, es probable que siga en curso de transmisión, aunque esté almacenado en el sistema. Es probable que el mensaje se almacene digitalmente en el servidor de la compañía telefónica y, por tanto, Bobby ha accedido a datos informáticos. ¿Es un teléfono un ordenador? Probablemente sí, ya que se encarga del tratamiento automatizado de los datos. Los agentes de policía que realizan registros y encuentran teléfonos pueden tener que considerar esto para asegurar que tienen la autorización necesaria para acceder a esos mensajes. Sería diferente si el destinatario hubiera escuchado el mensaje y hubiera optado por almacenarlo.  Este escenario plantea cuestiones similares a las del escenario anterior. Sirve para ilustrar lo que podría ser una situación bastante común que puede aplicarse igualmente a los agentes que, ejecutando una orden de registro, confiscan un ordenador que contiene tanto correo electrónico abierto como no abierto. También sirve para ilustrar que el delito establecido en virtud del Artículo 3 se aplica a todas las formas de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos. |
| **Estudio de caso 5**   * **Hechos / escenario**   Bobby está interesado en los ovnis y cree que el Gobierno ruso ha capturado una nave espacial alienígena que aterrizó en Siberia a principios del siglo XX. Visita un sitio de reclutamiento militar ruso que tiene un enlace a un sitio operado por la fuerza aérea rusa. El sitio de las Fuerzas Aéreas requiere una contraseña, pero utilizando una herramienta de descifrado de contraseñas consigue acceder a él. Pasa algún tiempo explorando el sistema y copia una serie de archivos. También intenta borrar todos los archivos de registro de su actividad para evitar que los rusos le identifiquen. A continuación, altera la portada del sitio para que muestre la imagen de un OVNI en lugar de la insignia de las Fuerzas Aéreas.  *¿Ha cometido Bobby un delito?* Preguntas *¿Puede el acceso no autorizado por sí mismo constituir un delito de ataque de integridad de los datos o del sistema?*  *¿Constituye un delito el hecho de borrar las pruebas del acceso no autorizado?*  *¿Debe causarse un daño grave al funcionamiento del ordenador para incurrir en responsabilidad penal?* Puntos de debate La finalidad de estas disposiciones es proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado.  Bobby no estaba autorizado a acceder a la página web de las Fuerzas Aéreas, que estaba protegida por una contraseña. Por lo tanto, el acceso constituiría un delito de acceso ilícito.  Bobby ha borrado los datos, los archivos de registro y las insignias de las Fuerzas Aéreas y, aunque tal vez haya generado los archivos de registro, no son suyos, ya que el sistema estaba configurado para registrar dicha actividad. No tiene derecho a borrarlos. Las Fuerzas Aéreas podrían querer saber quién tiene acceso a su sistema.  Al alterar la imagen de la portada ha borrado y añadido datos al sistema, lo que, aunque es poco probable que haya provocado la pérdida de información importante, sería una vergüenza para las Fuerzas Aéreas. Sin embargo, lo que es más importante, aunque Bobby pueda alegar que solo accedió al sistema para buscar información y que solo borró registros u otros datos sin importancia, ¿puede cualquier administrador de sistemas confiar en la integridad de los datos tras una intrusión tan ilegal?  Si se ha cometido un delito en estas circunstancias será una cuestión de interpretación local. Es posible que no se haya establecido el umbral de gravedad. Sin embargo, el administrador de sistemas probablemente se sentiría obligado a desconectar el sitio para determinar el efecto de la intrusión, especialmente si el sitio al que se ha accedido contiene datos confidenciales o sensibles o se utiliza en operaciones que, si fueran mal, pondrían en peligro al público, como un sistema responsable del funcionamiento de una central nuclear.  Si, por ejemplo, el sistema al que Bobby accedió es el que se utiliza para el funcionamiento de una central nuclear, ¿serían los delitos previstos en los artículos 4 y 5 adecuados para reflejar la gravedad de una intrusión de este tipo, que equivale a un ataque a las infraestructuras críticas nacionales? |
| **6. Estudio de caso 6** Hechos / escenario Un programa automatizado de correo electrónico spam envía cada día correos electrónicos no solicitados a miles de usuarios de todo el mundo. Si se abre el correo electrónico, se descarga un software en el ordenador del usuario. El software no hace nada que afecte al funcionamiento del ordenador del usuario, no adquiere datos del ordenador del usuario ni borra ningún dato ni causa ningún otro tipo de daño, pero significa que el ordenador del usuario es ahora un "zombi" que forma parte de una "red zombi" que el "controlador de robots" puede utilizar para llevar a cabo diversos tipos de actividad.  *¿Se ha cometido un delito contrario al artículo 4 o 5 por parte del responsable del envío del spam?*   * **Preguntas**   *¿Se ha producido un acceso no autorizado a la máquina del usuario? ¿Se han alterado datos en el equipo del usuario?*  *¿Se han producido daños en el equipo del usuario?*   * **Puntos de debate**   Aunque no se haya producido ningún daño, el programa informático provoca una alteración de los datos en el ordenador del usuario. Esta alteración no ha sido autorizada, ya que no se ha advertido al usuario ni se le ha pedido su consentimiento para la modificación de su ordenador. ¿Es ilegal el envío de spam en sí mismo o es una mera molestia? ¿Solo se convierte en ilegal cuando tiene una repercusión negativa?  ¿Qué pasaría si el correo electrónico de spam contuviera un archivo adjunto e invitara al destinatario a abrir el archivo adjunto diciendo "esto te va a gustar"?  Se podría argumentar que el destinatario ha elegido y, por tanto, ha consentido la descarga de datos en su ordenador. Sin embargo, la realidad es que cualquier consentimiento que se haya dado no ha sido un consentimiento informado, aunque se puede argumentar que aquellos que eligen abrir archivos adjuntos de destinatarios desconocidos lo hacen bajo su propio riesgo.  ¿Acaso importa que el usuario no se preocupe de que su ordenador pase a formar parte de la "red zombi" o no?  Cuando viajamos por Internet, visitamos sitios y descargamos datos sin tener en cuenta la naturaleza del material que puede llegar a nuestro ordenador, sino que confiamos en los nombres que se dan a sí mismos los sitios web, los nombres de los archivos o los resultados devueltos por nuestro motor de búsqueda para tomar nuestras decisiones. Hacer clic en una imagen en miniatura de una fotografía para adquirir una imagen a tamaño completo indica que somos conscientes de los datos que queremos adquirir y que damos nuestro consentimiento con pleno conocimiento de causa sobre la naturaleza de esos datos. Si hacemos clic en una imagen en miniatura de un automóvil solo para descubrir que la imagen de tamaño completo que hemos adquirido es la de un avión, no puede decirse que hayamos dado nuestro consentimiento a la adquisición de esos datos.  La elección de abrir un enlace a un sitio web dará lugar a la descarga de muchos datos. Si el sitio es legítimo, la mayor parte de los datos se referirá probablemente al contenido del sitio web, aunque una parte puede consistir en anuncios colocados por terceros. De nuevo, hemos tomado una decisión informada y hemos dado nuestro consentimiento implícito para recibir la publicidad, sabiendo que es una práctica común en Internet. Una práctica habitual en el sector de Internet es la descarga de datos en el navegador del usuario, las "cookies".  Las cookies desempeñan una serie de funciones, en particular el registro del historial de navegación del usuario. Un usuario tendrá la opción de desactivar la función de cookies en el navegador, ¿es esta opción suficiente para implicar que el usuario ha dado posteriormente su consentimiento a la descarga de dichos datos? |
| **7. Estudio de caso 7**   * **Hechos / escenario**   Bobby es un ex policía que fue despedido por el uso indebido del sistema informático de la Policía. Decide desquitarse con el departamento de policía. Utiliza un programa de correo electrónico que le permite enviar 70.000 correos electrónicos por hora a su antiguo departamento. Altera el encabezamiento del correo electrónico para que parezca que procede del jefe de la Policía y así engañar al servidor de correo electrónico de la Policía haciéndole creer que procede de una fuente legítima. El servidor de la Policía no pudo soportar el volumen de tráfico y se colapsó.  *¿Es esto un delito de ataque a la integridad del sistema?*   * **Preguntas**   Enviar un correo electrónico implica acceder o intentar acceder a un sistema informático, el servidor de correo electrónico. *¿En qué medida el propietario de dicho servidor autoriza dicho acceso?*  *Si uno tiene una dirección de correo electrónico, ¿no significa que está invitando a otros a enviarle mensajes de correo electrónico?*   * **Puntos de debate**   La cuestión es de derecho. Bobby ha accedido a un sistema y ha provocado el colapso de este introduciendo datos. Al establecer una dirección de correo electrónico accesible al público, el propietario de esta última está dando implícitamente su consentimiento a la recepción de mensajes. Bobby podría argumentar que la Policía ha consentido la recepción de cada correo electrónico individual y que no es su culpa que su sistema no tenga capacidad para manejar tantos mensajes. Pero, ¿ha habido realmente consentimiento? El propietario de una casa concede el consentimiento implícito para que el cartero pueda enviar a través de su buzón las cartas que van dirigidas al primero. También hay un consentimiento implícito para recibir correo "basura", como folletos de pizza. Sin embargo, el propietario no consiente en recibir tantos folletos de pizza hasta el punto de no que no pueda abrir la puerta de su casa.  ¿No podría decirse también que al alterar los datos del remitente del correo electrónico se ha obtenido acceso al servidor de correo electrónico mediante un fraude? No se da el consentimiento para la recepción de estos correos electrónicos "falsificados".  Aunque este escenario se refiere a los correos electrónicos, el principio es bueno para aquellos que buscan causar el colapso de los sitios web a través de un ataque de denegación de servicio por el que el sitio es incapaz de manejar el volumen de tráfico que se le dirige. La conexión a un sitio web implica el intercambio de datos entre el ordenador del usuario y el sitio web. Se plantean cuestiones similares en cuanto al consentimiento implícito para conectarse al sitio, tal y como se ha comentado en relación con los mensajes de correo electrónico. |
| **Estudio de caso 8**   * **Hechos / escenario**   Bobby envía un correo electrónico a su esposa, que se encuentra en su lugar de trabajo. Altera el encabezado para que parezca que proviene de una de sus amigas. El correo electrónico contiene un programa llamado "acceso a todas las áreas" que permite a Bobby asumir el control del ordenador de su mujer. Antes de que Bobby tenga la oportunidad de utilizar el programa, el administrador del sistema detecta su presencia y apaga el sistema para evaluar el alcance de la intrusión.  *¿Ha cometido Bobby un delito contrario al artículo 5?*   * **Preguntas**   ¿Ha provocado Bobby una supresión de los datos contenidos en el sistema? ¿Ha obstaculizado gravemente Bobby el funcionamiento de un sistema informático?  ¿Esta supresión de datos u obstaculización del funcionamiento del sistema se ha realizado de manera ilegítima?   * **Puntos de debate**   La respuesta del administrador del sistema al correo electrónico de Bobby significa que se ha negado el servicio a los usuarios del sistema. Por lo tanto, se ha suprimido el acceso a los datos del sistema, aunque es probable que la restricción de acceso sea temporal. El delito no requiere que los datos no estén disponibles de forma permanente.  Hemos discutido hasta qué punto el propietario de una dirección de correo electrónico otorga su  consentimiento para la recepción de datos de otros.  El artículo 5 se refiere a los sistemas informáticos, es decir, a uno o varios ordenadores conectados entre sí. ¿Se puede considerar como un sistema un único ordenador conectado a Internet?  El ordenador de trabajo de la mujer de Bobby es probablemente parte de un sistema, probablemente forma parte de una LAN (red de área local) o WAN (red de área amplia) o de una intranet. ¿Ha obstaculizado Bobby el funcionamiento del sistema?  Bobby podría argumentar que no es responsable de la denegación de servicio y que no tenía ninguna intención de provocar tal suceso; de hecho, todo lo contrario, quería que el sistema siguiera funcionando para poder averiguar lo que su esposa estaba haciendo. A menudo, los ataques de denegación de servicio no son suficientes para desconectar un sitio web, pero los proveedores de servicios lo desconectan para minimizar el efecto del ataque en sus sistemas y las molestias a otros clientes.  En este caso, Bobby no parece tener la intención necesaria para cometer un delito previsto en el artículo 5, aunque esto no significa, por supuesto, que escape a la responsabilidad penal.  Este es un ejemplo de un virus troyano, que es una forma habitual de que los ciberdelincuentes accedan a los ordenadores de otros. |
| **9. Estudio de caso 9**   * **Hechos / escenario**   Un grupo de "hacktivistas" en línea que protestan contra el uso de animales para la experimentación de cosméticos lleva a cabo ataques de "denegación de servicio distribuido" (DDOS) contra los sitios web de empresas de cosméticos y revistas de glamour. A través de su página web, el grupo distribuye un software que denominan "Supergun", que permite al grupo coordinar los ataques a los sitios web y maximizar así la cantidad de tráfico con la que desean acceder a un sitio web en un momento determinado. El software "Supergun" se desarrolló originalmente como una herramienta para que los administradores de sistemas comprobaran la seguridad de sus sistemas. Sin embargo, aunque el software sigue funcionando exactamente igual, la interfaz de usuario se ha hecho mucho más fácil de usar y ahora lleva el logotipo del grupo.  *¿Constituye un delito hacer que el software Supergun se pueda descargar? ¿Es un delito estar en posesión del software Supergun?*   * **Preguntas**   ¿El hecho de que Supergun se pueda utilizar para un fin legítimo significa que no se puede iniciar una acción judicial?  ¿El hecho de poner el software Supergun a disposición de los usuarios para su descarga equivale su distribución?   * **Puntos de debate**   Los delitos a los que se refiere este artículo son: acceso no autorizado, interceptación ilícita, ataque a la integridad de los datos y del sistema.  Aunque el software era originalmente de doble uso, es decir, tenía una función legítima, ahora que la interfaz de usuario ha sido modificada, ¿significa esto que su posesión, etc., constituye un delito?  Volviendo a nuestros estudios de caso anteriores, el software de "acceso a todas las áreas" utilizado por Bobby para acceder al ordenador de su esposa tiene un uso legítimo. Programas como este permiten a los usuarios acceder a sus propios ordenadores de forma remota. ¿Qué pasa con la posesión por parte de Bobby de un software para descifrar contraseñas; sería esto un delito? Puede ser una cuestión de intención, ¿qué razón legítima tiene para poseer dicho software? ¿Existe alguna prueba que demuestre que ha intentado utilizar este software para cometer un delito?  Este delito no está diseñado para ser utilizado para criminalizar a los proveedores y usuarios legítimos de software. Cuando, como ocurre en este caso, hay pruebas de una intención maliciosa, quizá no se plantee el problema. Sin embargo, los implicados en la ciberdelincuencia también suelen participar en actividades legítimas en Internet y pueden ser profesionales del sector que utilizan y desarrollan dicho software pero que, cuando se presenta la oportunidad, están dispuestos a utilizarlo para promover actividades ilegales. ¿Cómo se supone que van a saber qué intención tiene un cliente en relación con un determinado equipo o programa informático? ¿Es el ámbito del delito demasiado vago? |
| **Estudio de caso 10**   * **Hechos / escenario**   Un proveedor de software ha creado un software de cifrado. El software divide el contenido del disco duro en dos volúmenes, cada uno de los cuales requiere una contraseña de acceso, pero solo un volumen es visible para el usuario ordinario y la existencia del volumen oculto no puede detectarse utilizando el software forense disponible en la actualidad.  El fabricante afirma que este software sería de uso para cualquier persona que se encuentre en una situación en la que esté coaccionada para revelar su contraseña. Significaría que los datos del volumen oculto pueden mantenerse seguros incluso si revelan la contraseña de la carpeta visible.   * **Preguntas**   ¿Constituye la fabricación, producción, distribución, uso o posesión de este tipo de software un delito?   * **Puntos de debate**   A todos se nos insta constantemente a mantener nuestros datos seguros. Aunque es evidente que un programa de este tipo es útil para quienes se dedican a la delincuencia y, en particular, para quienes temen que el contenido de sus ordenadores pueda incriminarles, el programa no se utiliza para cometer un delito, sino para ocultar pruebas.  Los ciberdelincuentes pueden hacer uso de otros programas o sistemas para evitar ser detectados, en particular anonimizadores que les permiten navegar por Internet sin revelar su verdadera dirección IP o programas de eliminación de pruebas que pueden borrar el contenido de un disco duro. |
| **Estudio de caso 11**   * **Hechos / escenario 3**   Nick trabaja en el departamento de informática de una gran empresa que tiene su propia intranet. La política de la empresa prohíbe a sus empleados utilizar el ordenador de la empresa y la conexión a Internet para realizar compras en línea. En su tiempo libre, Nick empieza a desarrollar un programa informático que permita a la empresa identificar a los empleados que realizan pagos en línea y capturar esa información para poder utilizarla como prueba en un procedimiento disciplinario. Nick carece de los conocimientos necesarios y se pone en contacto en línea con "Júpiter". Juntos desarrollan un programa informático que, una vez descargado en el ordenador del usuario, se activa cuando este comienza a cumplimentar un formulario en línea, como el utilizado para procesar los pagos en línea, y captura los datos que se introducen. La empresa de Nick está muy satisfecha mientras Júpiter comienza a desplegar el software utilizando un programa troyano.  *¿Ha cometido Nick un delito?*  *¿Ha cometido la empresa un delito? ¿Ha cometido Júpiter un delito?*   * **Preguntas**   ¿Se ha diseñado o adaptado el dispositivo principalmente con el fin de cometer determinados delitos?   * **Puntos de debate**   Los ciberdelincuentes pueden acceder a una serie de herramientas que les permiten cometer delitos o que les ayudarán a hacerlo. Es posible adquirir el código que le permitirá construir su propio "zombi" o comprar una "red de zombis" o acceder a una red de zombis que permitirá al usuario llevar a cabo diversos tipos de delitos como el "phishing”.  Júpiter utilizará este programa para obtener información financiera de los usuarios que puede ser explotada por el propio Júpiter o por otros. Es de suponer que la empresa pensó que Nick había generado mientras estaba trabajando. Nick es inocente y ha ayudado inadvertidamente a Júpiter a crear una poderosa herramienta criminal. Ni Nick ni la empresa tienen la intención criminal requerida. ¿Sería diferente si Júpiter comercializara el programa a otras empresas que quisieran controlar la actividad de sus empleados en Internet? ¿Podría argumentar Júpiter que el programa tiene una finalidad legítima a pesar de su evidente atractivo para los delincuentes? |
| **Estudio de caso 12**   * **Hechos / escenario**   Stefan utiliza un software fotográfico disponible en el mercado para producir una letra bancaria realista en el ordenador de su casa. Lleva la letra bancaria a su banco, que la acepta como auténtica y transfiere los fondos a la cuenta de Stefan.  *¿Qué delito ha cometido Stefan?*   * **Preguntas**   ¿Es la producción de la letra bancaria falsificada una falsificación informática?  ¿El delito solo se cumple cuando el empleado del banco acepta la letra bancaria como auténtica?   * **Puntos de debate**   La creación de la letra bancaria implica la introducción de datos no auténticos en un ordenador,  es decir, que la letra bancaria ha sido emitida a favor de Stefan. Sin embargo, ¿se ha hecho de manera ilícita o tiene Stefan derecho a elaborar dicho documento en su propio ordenador? Stefan puede tener la intención de utilizar la letra bancaria para defraudar al banco, pero, por la razón que sea, nunca llega a imprimirla. ¿Influye en la responsabilidad de Stefan el hecho de que el documento se presente en papel?  Este delito no se creó realmente para tratar este tipo de escenario, aunque puede servir si la legislación nacional no criminaliza de otro modo la producción de una letra bancaria falsificada. Estos delitos pueden considerarse mejor en términos de responsabilidad secundaria, como la tentativa.  Este delito está realmente dirigido a aquellos que utilizan un ordenador como mecanismo para cometer el delito, por lo que cuando actúa de buena fe el empleado del banco introduce los datos suministrados por Stefan aceptando que son auténticos. |
| **Estudio de caso 13**   * **Hechos / escenario**   Stefan siempre ha presumido ante sus amigos de sus proezas como atleta cuando era adolescente. Sus amigos se muestran escépticos. Consigue acceder a la base de datos de su antiguo colegio y altera los registros para que aparezca como capitán del equipo de atletismo del colegio y que ha ganado varias medallas.  *¿Se trata de un delito de falsificación informática?*   * **Preguntas**   Los datos que se han alterado no se utilizarán para ningún fin legal.   * **Puntos de debate**   Stefan ha alterado los datos y ha introducido datos que no son auténticos. Está claro que este acceso y alteración se han cometido de manera ilegítima. Dejando a un lado los otros delitos que pueda haber cometido Stefan, es dudoso que haya cometido una falsificación informática, ya que estos datos no se utilizarán con fines legales.  El delito relacionado con la falsificación no tiene que ver con el beneficio económico o de otro tipo; esos delitos entran en el ámbito del fraude informático. Este artículo pretende asegurar la seguridad y la fiabilidad de los datos electrónicos que pueden tener consecuencias para las relaciones legales. La expresión "a efectos legales" se refiere a las transacciones y documentos legales que son relevantes desde el punto de vista jurídico. |
| **Estudio de caso 14**   * **Hechos / escenario**   Ahora que ha perdido su trabajo en el cuerpo de policía y tiene que pagar la pensión alimenticia a su mujer desde su divorcio, Bobby busca otra forma de ganar dinero. Siempre le ha interesado el comercio de acciones y compra 1.000 acciones de Flanders Mining Inc, una empresa con derecho exclusivo a extraer uranio en Bélgica, por 1 euro cada unidad. Bobby es miembro de un foro de Internet cuyos miembros están, como Bobby, interesados en la bolsa. Bobby publica un mensaje en el que dice que un amigo del Gobierno belga le ha comunicado que se han detectado importantes cantidades de uranio en Bélgica. Tras este anuncio, la cotización de las acciones de Flanders Mining se dispara, y al final de la semana cada acción vale 1.000 euros. Bobby vende entonces sus acciones.  *¿Ha cometido Bobby un delito?*   * **Preguntas**   ¿Es el mensaje de Bobby falso?  Si el mensaje era falso, ¿ha perdido otra persona su propiedad como resultado? ¿Ha obtenido Bobbie una ventaja económica?   * **Puntos de debate**   Si el mensaje publicado por Bobby es falso, puede haber cometido un delito. Ha introducido datos falsos en un ordenador y ha obtenido un beneficio económico por la subida del precio de las acciones.  ¿Existe una relación de causalidad entre la introducción de los datos y el efecto a distancia?  ¿Ha causado Bobby una pérdida para otros? Podría decirse que sí, ya que las acciones están mal valoradas y es de suponer que en algún momento bajarán. Sin embargo, hay que reconocer que el mercado de las acciones es extremadamente volátil, ¿no es el valor  de una acción el precio que cualquiera está dispuesto a pagar? ¿Realmente se ha defraudado a alguien, no abundan este tipo de rumores y mensajes en Internet? ¿realmente alguien va a creer este post o no lo va a ver como un torpe intento de manipular el precio de las acciones? ¿Significa esto que no podemos decir mentiras en Internet? |
| **Estudio de caso 15**   * **Hechos / escenario**   Stefan se dirige al banco. En el aparcamiento se da cuenta de que le falta cambio. Pone una arandela en la máquina automática de aparcamiento y obtiene un tique.  *¿Ha cometido Stefan un delito?*   * **Preguntas**   ¿Es la máquina de aparcamiento un ordenador?  ¿Importa que la máquina de aparcamiento produzca tiques automáticamente y que no se haya engañado a ningún ser humano?  ¿Cómo debe considerarse el tique de aparcamiento?   * **Puntos de debate**   La máquina de aparcamiento es un ordenador, procesa los datos calculando la cantidad de dinero que se proporciona en relación con la tarifa de aparcamiento y expende un tique por el tiempo apropiado. Stefan ha introducido datos no auténticos, la arandela en lugar de la moneda adecuada. El artículo 7 no exige que una persona haya modificado los datos suministrados.  El tique de aparcamiento es una falsificación, los datos utilizados para crearlo eran falsos y se produjo con el fin de que una persona, el encargado del aparcamiento, lo considerara auténtico y diera a Stefan un tique de aparcamiento. |
| **Estudio de caso 16**   * **Hechos / escenario**   Tras su detención, la policía descubre que Stefan está en posesión de los datos de las tarjetas de crédito de un gran número de terceros.  *¿Constituye la posesión de estos datos un delito?*   * **Preguntas**   ¿Cómo deben considerarse los archivos informáticos? ¿Son "cosas" desde el punto de vista jurídico, a pesar de que lo único que contienen es una cadena de código binario?   * **Puntos de debate**   En el Reino Unido es un delito penal sustantivo estar en posesión de un artículo para utilizarlo con fines fraudulentos. El artículo incluye un archivo informático. Por supuesto, es necesario demostrar la intención necesaria, pero es difícil argumentar una razón legítima para tener la posesión de datos de este tipo.  Es posible que se considere un delito preparatorio. |
| **Estudio de caso 17**   * **Hechos / escenario**   Adam es miembro de un grupo exclusivo en línea que intercambia fotografías de niños de los que se abusa sexualmente. Es también miembro de un grupo de intercambio de archivos "peer to peer", coloca las fotografías de niños víctimas de abusos que ha obtenido del grupo en línea en estas carpetas compartidas con la modalidad peer to peer, lo que las hace accesibles a otros miembros de la red.  *¿Qué delitos ha cometido Adam?*   * **Preguntas**   Definiciones de producción, adquisición y distribución.  Adam ha descargado archivos de imagen de Internet. ¿La descarga equivale a la producción de dicha imagen? Descargar, y en particular guardar una imagen en un ordenador, no es como ver la televisión. El acto de descargar crea una cosa nueva, un archivo informático, por lo que ver imágenes en Internet implica la creación de nuevas imágenes. Los fiscales pueden encontrar útil este concepto.  Las redes de intercambio de archivos Peer to Peer permiten a sus miembros acceder a los archivos que otros miembros de la red ponen a su disposición. Al colocar las imágenes en la carpeta compartida, Adam las pone a disposición para su distribución. |
| **Estudio de caso 18**   * **Hechos / escenario**   Bill es detenido en el aeropuerto a su regreso de Camboya. Se descubre que su ordenador portátil contiene un gran número de imágenes en las que aparece realizando actividades sexuales con niños que parecen ser del sudeste asiático.  *¿Se puede procesar a Bill por las imágenes?*   * **Preguntas**   Jurisdicción.  Elección del delito de fondo, estar en posesión de una imagen o producir la imagen.   * **Puntos de debate**   Puede haber problemas de jurisdicción en relación con la producción de las imágenes, ya que estas parecen haber sido producidas en el extranjero.  La posesión no debería ser un problema. |
| **Estudio de caso 19**   * **Hechos / escenario**   [WWW.Iuvfishin.com](http://WWW.Iuvfishin.com/) es un sitio web dedicado a la pesca. El sitio está alojado en servidores ubicados en EE.UU. Los propietarios del sitio descubren que ha sido pirateado y que se han cargado e incrustado en el sitio mil imágenes de abusos a menores. Esto se ha llevado a cabo de modo que los usuarios ordinarios del sitio no puedan verlas. El sitio registra las direcciones IP de quienes han accedido a las fotografías.  Una dirección IP atribuida a John ha sido facilitada a la Policía de su país, que registra dicha dirección y confisca su, que contiene miles de imágenes de abusos a menores. Del historial de Internet y de los datos que contienen estos archivos se desprende que la mayoría de las imágenes han sido descargadas de Internet.   * **Preguntas**   ¿Cómo probar que John es responsable de las imágenes? Repercusión en los sospechosos acusados de delitos de pederastia.   * **Puntos de debate**   Este método de ocultación de imágenes no es infrecuente. Los grupos publican enlaces a las imágenes. Sin embargo, puede ser peligroso basarse únicamente en la dirección IP para obtener una orden de registro sin entender cómo esa dirección IP llegó a registrarse en el sitio, podrían haber llegado a él de forma totalmente inocente habiendo sido remitidos por otro sitio y no haber continuado para acceder a ninguna imagen una vez que se dieron cuenta de lo que eran. Por supuesto, es posible que lo hayan visitado en más de una ocasión o que hayan accedido a varias imágenes.  Se puede usar esto para discutir la precaución con la que se debe proceder antes de acusar a un individuo de ser un pedófilo. Hay un alto índice de suicidio entre las personas acusadas de estos delitos. Como en todos los casos de ciberdelincuencia, hay que poder situar al sospechoso ante el teclado en el momento pertinente, una dirección IP puede ser utilizada por varios individuos en la misma dirección o la red inalámbrica puede haber sido secuestrada por otra persona. Acusaciones de este tipo pueden tener un efecto devastador en un individuo inocente. |
| **Estudio de caso 20**   * **Hechos / escenario**   La Policía de EE.UU. ha desmontado un sitio web que aloja páginas que ofrecen imágenes de abusos a menores para quienes pagan una suscripción mensual. Las autoridades estadounidenses han capturado los datos de quienes han pagado por el acceso, en particular la dirección IP, los números de las tarjetas de crédito, la dirección de correo electrónico, la dirección de facturación y la contraseña. Uno de los clientes es Oswald. Tras obtener una orden de registro, se examina su ordenador. No se encuentra nada incriminatorio porque Oswald ha utilizado un programa llamado "Eliminación de pruebas".  *¿Ha cometido Oswald un delito?*   * **Preguntas**   ¿Ha cometido Oswald un delito de fondo o uno de responsabilidad secundaria? ¿Hay problemas de jurisdicción?  ¿Importa que el sitio web de EE.UU. estuviera totalmente automatizado?  ¿Qué se puede decir sobre el uso del programa de eliminación de pruebas?   * **Puntos de debate**   Oswald no está en posesión de ninguna imagen y no podemos probar que haya accedido alguna vez a un sitio web para ver dichas imágenes, aunque sí podemos probar que pagó una suscripción para hacerlo. Sin embargo, Oswald ha pagado dinero para persuadir a otra persona, el propietario del sitio web en EE.UU., para que distribuya o ponga a disposición imágenes de abuso infantil para su distribución. ¿Constituye esto un delito?  El hecho de que el sitio web de EE.UU. esté totalmente automatizado significa que no hay ningún ser humano que intervenga en el procesamiento de los datos de la tarjeta de crédito. Aun así, el proceso ha sido creado, administrado y mantenido por una persona que se beneficia económicamente.  El uso de un programa de eliminación de pruebas no es, per se, ilegal. A menos que Oswald haya podido activar el programa en el curso de la investigación policial, es poco probable que haya cometido un delito relacionado con la  administración de justicia. Sin embargo, si Oswald es procesado, el uso de estos programas puede ser considerado como un agravante por parte del tribunal. |