El cibercrimen en el ámbito económico y patrimonial

Prof. Dr. iur Dr. med. Carlos María Romeo Casabona
Prof. Dr. Iñigo de Miguel Beriain

Guía Docente

Datos de la asignatura

Nombre: El cibercrimen en el ámbito económico y patrimonial

Departamento: Departamento de Derecho Público y Cátedra Interuniversitaria, Diputación Foral de Bizkaia, de Derecho y Genoma Humano, Universidad del País Vasco / EHU.

Responsables: Prof. Dr. iur Dr. med. Carlos María Romeo Casabona (Catedrático de Derecho Penal y Director de la Cátedra Interuniversitaria de Derecho y Genoma Humano).

Prof. Dr. Iñigo de Miguel Beriain (Investigador de la Cátedra Interuniversitaria de Derecho y Genoma Humano en la Universidad del País Vasco/EHU).

Sumario de esta Guía Docente

1. Presentación de la asignatura

2. Objetivos a

3. Competencias

4. Prerrequisitos

5. Descripción y temario de la asignatura

5.1. Descripción y temario

5.2. Materiales básicos y complementarios

6. Metodología

7. Evaluación de la asignatura: autoevaluación

8. Cronograma

1. PRESENTACIÓN DE LA ASIGNATURA

Los llamados delitos informáticos empezaron a preocupar seriamente a partir de los años ochenta, no sólo como un fenómeno criminal nuevo necesitado de identificación y comprensión, sino también como cuestión jurídica, a la vista de su problemático encaje en los delitos existentes en los códigos penales de la época. Las oportunas reflexiones técnico-jurídicas y de política-criminal dieron lugar a la introducción en aquéllos de nuevas figuras delictivas que pudieran hacer frente a este nuevo fenómeno criminal: protección de datos personales, fraude informático, espionaje y sabotaje informáticos, etc. Este proceso normativo también tuvo lugar en España, pero quizá de forma más débil y por medio de una reforma legal relevante, pero algo

tardía, pues ésta sólo se produciría con la aprobación del Código penal de 1995.

Mientras tanto, la incorporación masiva de las tecnologías de la información y de la comunicación (TIC) y en particular de las redes telemáticas, principalmente Internet, como red abierta, a la vida cotidiana y su fácil accesibilidad por cualquier persona, han provocado un nuevo giro y nuevas manifestaciones de la criminalidad cibernética (el cibercrimen o ciberdelito), la cual no siempre encuentra respuestas jurídicas adecuadas con el fin de prevenir o sancionar su desarrollo. Conductas como los accesos ilícitos a datos e información ajenos circulando a través de la red (desde el correo electrónico y las conversaciones escritas u orales –*chat*- hasta el mero acceso o consultas a sitios de la red) o a bases de datos ubicadas en ficheros informáticos privados o pertenecientes a organismos públicos, constituyen un conjunto de delitos que pueden tener gran relevancia. Algunas de estas conductas han adquirido una trascendencia particularmente importante en el mundo económico y financiero y más concretamente en el ámbito de la empresa, que conocen así nuevas y diversas formas de agresión. En este contexto también es de gran interés jurídico-penal conocer los abusos que se cometen por parte de proveedores y clientes en las transacciones comerciales en la red, cada vez más extendidas, la responsabilidad que se quiere imponer o que ya se ha impuesto a los proveedores de acceso a la red y a otros servicios de la misma, la dificultad de determinar cuándo es aplicable la ley interna de un Estado determinado y, en consecuencia, la competencia de los tribunales de ese Estado, son algunos de los numerosos problemas que se están planteando en los últimos tiempos y que no siempre tienen fácil solución, sin perjuicio de algunas reformas del Código Penal más recientes.

Por consiguiente, es fácil comprender cuán importante es profundizar en estos temas con el fin de contribuir a su tratamiento jurídico-penal adecuado y de encontrar soluciones (en su caso, incluyendo las reformas oportunas de las leyes penales y procesales), en particular respecto a las actividades más vinculadas con el sector económico y empresarial. No cabe duda tampoco del interés que estos temas despiertan en la población, no sólo por su novedad, sino, sobre todo, porque de algún modo

y al menos potencialmente, todos podemos vernos involucrados como víctimas en algunas de estas conductas, aunque sea involuntariamente, lo que genera en los ciudadanos un sentimiento de inseguridad y de vulnerabilidad.

2. OBJETIVOS

A través de esta asignatura, **El cibercrimen en el ámbito económico y patrimonial**, que hemos denominado así para no circunscribirnos tan sólo a las actividades realizadas en o por medio de las TIC relacionadas con la empresa, sino también con la actividad económica y financiera en general, se pretende ofrecer al alumno/a un panorama de los aspectos jurídico-penales (pero también, aunque en menor medida, procesales y de Derecho Internacional) más relevantes relacionados con estas formas de criminalidad, especialmente en sus manifestaciones más novedosas, y cuáles son las respuestas jurídicas que a este respecto se han establecido. En este panorama no puede dejar de ofrecerse una breve exposición criminológica de este fenómeno, esto es, de cuáles son sus manifestaciones actuales más representativas en el sector señalado, y cómo actúan sus autores y qué perfiles presentan éstos, pues sólo con tales antecedentes podrá abordarse su estudio jurídico-dogmático y político-criminal.

En consecuencia, a grandes rasgos podemos considerar dos los objetivos perseguidos con la presente asignatura:

a) En primer lugar, aproximar al alumno a los problemas y debates fundamentales que las formas de criminalidad relacionadas con las TIC (sobre todo internet, pero también redes intranet y otras) plantean al Derecho Penal, tanto en algunas categorías generales (Parte General: aplicación de la ley penal, teoría del delito) como en los delitos específicos más directamente relacionados con el sector económico y patrimonial y el mundo de la empresa (Parte Especial: delitos de espionaje industrial y contra la libre competencia empresarial, fraude informático, falsedad documental, propiedad intelectual, etc.) y otros delitos no directamente relacionados con este sector social pero que

pueden ser instrumentales en el mismo (acceso a datos de carácter personal, interceptación de las comunicaciones, suplantación o "robo" de identidad, intrusión o acceso no autorizado a archivos o bases de datos, etc.). También se apuntan algunas perspectivas criminológicas generales de este fenómeno delictivo.

b) Conocer las soluciones articuladas hasta el momento por el Derecho Penal internacional e interno para cada una de las cuestiones que suscita el cibercrimen y otros delitos informáticos en el ámbito aludido.

De todos modos, no es suficiente con este enfoque, pues a la vista de la potencialidad y constante desarrollo que ofrecen las TIC debe dotarse al alumno/a del instrumental teórico-jurídico necesario para hacer frente a los futuros retos que se plantearán en este campo al jurista.

Con esta iniciación a una forma novedosa pero también creciente de la delincuencia se quiere contribuir a la formación de expertos en esta materia en el marco más amplio del Derecho de la empresa, pues es previsible que se experimente una mayor demanda social de esta preparación en los próximos años.

3. COMPETENCIAS

Una vez terminado el estudio de esta asignatura, quien lo haya realizado con interés y aprovechamiento podrá:

- Identificar en qué consisten los ciberdelitos y deslindar con precisión cuál es el ámbito real de estos delitos.
- Conocer cuáles son los principales problemas de adscripción jurídica que plantean y cómo resolverlos, sobre todo desde su dimensión transfronteriza, que es probablemente la más compleja.
- Identificar con precisión cuáles son las necesidades de armonización legal y cooperación jurisdiccional y policial

de estos delitos en el marco internacional y supranacional europeos.

- Conocer cuáles son los delitos relacionados con las TIC que figuran en la legislación penal española, ayudando a su interpretación y aplicación, contando como apoyo a este respecto, cuando ello es posible, con las decisiones judiciales más importantes. Sin perjuicio de un acercamiento comparado cuando ello es oportuno.

La capacidad global que debería adquirirse será, en suma, la de un experto de nivel medio-alto sobre los aspectos jurídico-penales de los ciberdelitos y de los delitos relacionados con las TIC en general.

4. PRERREQUISITOS

La asignatura **El cibercrimen en el ámbito económico y patrimonial** está concebida para ser cursada mediante el sistema establecido por el *Proyecto OpenCourseWare* (OCW). El interés que despierta este nuevo y peculiar fenómeno criminal permite ser cursada por estudiantes universitarios con un perfil diverso, como son, en primer lugar, los relacionados con el Derecho y con la informática (Ingeniería informática, etc.); pero igualmente los de Ciencias de la Información, de la Administración, Empresariales, Económicas, etc. En todo caso, es compatible con cualquier perfil académico. Por ello no es exigible ningún prerrequisito

Para cursar la presente asignatura no es necesario, por consiguiente, haber cursado previamente otros estudios universitarios específicos. Sin embargo, será probablemente más asequible para estudiantes de Grado de Derecho que al menos hayan superado las asignaturas relacionadas con la Parte General del Derecho Penal.

Teniendo presente la circunstancia de que la asignatura puede ser cursada por alumno con formación de base diferente, se ha procurado limitar en lo posible el uso de lenguaje jurídico muy técnico, así como el manejo de algunos conceptos fundamentales

del Derecho Penal, aunque es inevitable que ambos estén presentes. Los alumnos/as que necesiten alguna aclaración de este tipo deben hacer las consultas que necesiten a lo largo del curso.

5. DESCRIPCIÓN Y TEMARIO DE LA ASIGNATURA

5.1. Descripción y temario

Además de la presentación introductoria de la asignatura, realizada más arriba, en el apartado 1º, puede añadirse ahora que los contenidos de la asignatura se corresponden con los del programa de la misma, cuya extensión se ha calculado en atención a la carga de créditos que aquella tiene asignada. Comprende los siguientes temas, a los que se acompaña una breve descripción o sinopsis, de modo que se pueda adquirir una idea general de los contenidos.

Tema 1º
Aspectos generales sobre la cibercriminalidad y el cibercrimen
Las formas de aparición del cibercrimen.
La vulnerabilidad de las TIC.
¿Delitos informáticos o ciberdelitos?
Este tema constituye una primera aproximación a la problemática del ciberdelito y trata de presentar los conceptos iniciales vinculados con el mismo. El objetivo consiste en familiarizar al alumno/a con el concepto de ciberdelito y con las cuestiones más generales que desde el punto de vista jurídico-penal suscita.

Tema 2º
Los criterios de intervención del Derecho Penal frente al ciberdelito
Los sujetos del ciberdelito.
La aplicabilidad efectiva de la ley penal.
Procedimientos de entreayuda judicial. Obtención de elementos probatorios
En primer lugar, se contemplan los aspectos más relevantes relacionados con los potenciales sujetos del delito (p. ej., las

personas jurídicas como sujetos activos o perpetradores del delito; o las personas inexistentes como sujetos pasivos o víctimas del delito).
Se presentan también los conceptos básicos ligados con las cuestiones de jurisdicción y de competencia más peculiares del espacio virtual: limitaciones que comporta para estos delitos la aplicación del principio de territorialidad, determinar la jurisdicción competente y otros aspectos de entreayuda judicial, como la extradición.
Se menciona finalmente el recurso a las TIC para la obtención de pruebas de inculpación de presuntos delincuentes investigados (interceptación de las comunicaciones con autorización judicial).

Tema 3º
Accesos no autorizados a los sistemas y ficheros informáticos (I)
Aspectos generales.
La protección penal de los datos y de las comunicaciones personales a través de la red. El caso de las personas jurídicas (empresas).
Comunicaciones privadas en el ámbito laboral de la empresa.
A lo largo de los últimos años se ha informado con relativa frecuencia en los medios de comunicación sobre conductas relacionadas con los accesos no autorizados a los sistemas informáticos. El objetivo de este tema es analizar dichas conductas y determinar la relevancia penal de las mismas, dedicándose especial atención a las interferencias de las comunicaciones privadas (mensajes de correo electrónico, accesos a foros en la red, etc.), que pueden tener un contenido empresarial y financiero, y de forma específica de las comunicaciones en el lugar de trabajo.

Tema 4º
Accesos no autorizados a los sistemas y ficheros informáticos (II)
Espionaje industrial y agresiones al secreto de empresa a través de la red.
Interferencias en sistemas informáticos
Daños en sistemas y ficheros informáticos. Ciberterrorismo.
Diversas conductas llevadas a cabo a través de la red, así el espionaje industrial o de empresa, han ido adquiriendo una

creciente y muy significativa importancia, dada la intensidad con la que las mismas pueden atacar el bien jurídico secreto de empresa, base de la competitividad en este sector productivo. Otros comportamientos, como el daño y el sabotaje informáticos o, incluso, el ciberterrorismo (éste tan solo desde su repercusión en la empresa), deben asimismo ser analizados desde la óptica del Derecho Penal, al objeto de calibrar su carga real de ofensividad.

Tema 5º
Manipulaciones en sistemas y ficheros informáticos (I)
El fraude informático.
Las transacciones a través de la red y de terminales bancarios.
Asistimos en la actualidad a una proliferación enorme de transacciones financieras y comerciales realizadas a través de las TIC y, en particular, de algunos terminales, por ejemplo, bancarios, de manera que una parte muy significativa de las operaciones de compra-venta u otras financieras se materializan sin presencia de dinero físico (dinero electrónico). El objetivo de este tema es analizar la relevancia penal de las conductas de fraude informático y otras similares, cuya importancia patrimonial resulta indudable, diferenciándolas al mismo tiempo de las estafas y otros fraudes ajenos al medio.

Tema 6º
Manipulaciones en sistemas y ficheros informáticos (II)
Falsedades documentales.
Piratería informática
La protección penal de los sistemas lógicos y de los productos multimedia.
En este tema se analiza un conjunto heterogéneo de conductas. Las primeras se caracterizan por la alteración, con diversos propósitos, de datos informáticos o de archivos que pueden gozar del reconocimiento de documento en las relaciones jurídicas aplicables a la actividad empresarial.
El alcance de la protección penal y no penal de los programas de ordenador y otros productos lógicos, así como la facilidad de acceso y copia a través de la red de otros productos de multimedia (música, imágenes, películas, textos literarios y técnicos, etc.), ha generado un intenso debate social, que enfrenta

a productores, autores y consumidores, a la que no debe ser ajena el legislador. El objetivo de este tema es exponer la respuesta penal producida ante este tipo de conductas, pero como se verá, aquí la función del Derecho Penal es secundaria o residual en relación con otros sectores del ordenamiento jurídico (p. ej., legislación sobre propiedad intelectual).

Lección 7ª
Hacia un nuevo Derecho Internacional y Europeo contra el cibercrimen
El Convenio Europeo sobre Cibercrimen y los delitos de carácter patrimonial.
El Derecho supranacional de la Unión Europea.
Conclusiones de política legislativa.
El cibercrimen como conducta delictiva que se lleva a cabo fundamentalmente desde un entorno global (las TIC, y en particular, la red de redes, Internet) precisa igualmente de una respuesta conjunta desde los ámbitos europeo e internacional. El objetivo de este tema es presentar al alumno/a las características de este esfuerzo para ofrecer una respuesta adecuada y coordinada a dichas conductas.

5.2. Materiales básicos y complementarios

Las fuentes documentales serán tanto teóricas (incluirán todo el temario descrito más arriba) como vinculadas a las actividades aplicativas (supuestos prácticos o preguntas relacionados con los diversos temas y con hechos delictivos, que deberán ser resueltos, y figuran incluidos al final de cada uno de ellos).

Los materiales han sido elaborados por el Prof. Carlos María Romeo Casabona, con la colaboración del Prof. Iñigo de Miguel Beriain.

6. METODOLOGÍA

En primer lugar, y a fin de facilitar la comprensión de la metodología de la asignatura, deben subrayarse las oportunidades, herramientas y condicionantes derivados de la oferta de la asignatura en el OCW.

Dado que el contacto profesor-alumno/a se produce exclusivamente por vía de los materiales de estudio, de actividades aplicativas y ejercicios y otros materiales de consulta, el alumno/a deberá redoblar los esfuerzos con el fin de suplir la ausencia de relación directa entre docentes y discentes. El Campus Virtual de la Universidad del País Vasco/EHU dispone de una serie de mecanismos articulados con el fin de lograr aproximar a tutores y alumnos/as. Deberá prestarse especial atención a los criterios necesarios para la optimización del tiempo empleado en la preparación de la asignatura por parte del alumnado y cumplir los planes de estudio y de actividades que se indican en el cronograma.

Por tal motivo, es muy importante que el alumno/a mantenga un acceso periódico constante a la plataforma de la asignatura en el OCW, o, en su caso, a todos los materiales puestos a su disposición. Se pretende así que el alumno/a realice sus trabajos sobre una serie de supuestos práctico-aplicativos, que deberá resolver al final del estudio de cada tema, siendo la resolución de los mismos un factor muy relevante para asegurar la efectividad del estudio, el acceso periódico regular a la asignatura y así lograr la comprensión y asimilación de los conocimientos que garanticen el logro de las competencias propuestas.

Básicamente, la preparación de la asignatura se estructura en dos niveles, con materiales diversos:

El adecuado conocimiento de la parte teórica de la asignatura resulta a todas luces imprescindible para superar con éxito la evaluación continuada. Los temas concluyen con unas preguntas que serán contestadas por el alumno/a, de acuerdo con el procedimiento que se indica más abajo.

Junto con el material de la parte teórica se encuentran las actividades aplicativas, que se desglosan en la solución de los supuestos prácticos que se plantean y en la contestación a preguntas aplicadas en relación con cada tema en particular. A esta herramienta deben acceder los alumnos/as una vez finalizada la preparación del correspondiente tema. El interés de los mismos es doble: por un lado, permiten al alumno/a profundizar en el

estudio de la asignatura, y por otro, constituye la base para el procedimiento de autoevaluación por parte del propio alumno/a.

En todo caso, como *Trabajo final*, una vez terminado todo el temario, el alumno/a debería elaborar un informe sobre su visión personal de conjunto del contenido global de la asignatura (*El cibercrimen en el ámbito económico y patrimonial*) y de los problemas jurídicos más relevantes en su opinión y las soluciones globales que podrían articularse por las instancias oportunas.

7. EVALUACIÓN DE LA ASIGNATURA: AUTOEVALAUCIÓN

Dadas las características específicas del sistema OCW, en particular su carácter no presencial como procedimiento docente y de estudio, es decir, el uso de herramientas virtuales, se impone el procedimiento de autoevaluación, es decir, corresponde al propio alumno evaluar sus actividades de aprendizaje. La autoevaluación es difícil, pues exige al alumno honestidad en asumir los resultados reales obtenidos, disciplina y regularidad en el proceso periódico de autoevaluación, lo que requiere a su vez una disciplina observancia del cronograma para mantener de forma constante y regular las actividades de estudio y las aplicativas. El alumno debería asumir la realización de autopruebas escritas sobre algunas partes de los materiales relativos a la parte teórica, sin consultarlos durante el momento de contestación escrita.

Del mismo modo debería proceder cuando realice las actividades aplicativas que se proponen para cada tema. Habría que realizar *todos* los trabajos relacionados con *todos* los temas que configuran el Programa de la asignatura. Los criterios de autoevaluación, para lo que el alumno/a deberá contrastar lo contestado con los materiales de estudio disponibles, tendrán en cuenta el acierto en la resolución de los mismos, así como la seriedad, reflexión y redacción de las respuestas.

El trabajo final, sí podría realizarse consultando, tantas veces como se estime necesario, los materiales de estudio que han sido entregados, en particular los relativos al temario.

Si bien el conjunto del temario intenta asumir una perspectiva jurídica de carácter general, sin vinculación a un sistema jurídico determinado, es cierto que en relación con algunos principios y sobre todo con algunos delitos, se toma como referencia el Derecho penal español y el Derecho europeo. Si el alumno/a es de origen o residencia en un país diferente, se recomienda que las respuestas a las Actividades aplicativas se haga desde la perspectiva que se hace en los contenidos y materiales de cada Tema. A continuación sería muy útil y recomendable que el alumno/a contestara a las mismas preguntas desde la perspectiva del Derecho del país de su nacionalidad y/o residencia distintas del la española. Obrando así obtendrá el máximo rendimiento.

Resumiendo, el alumno/a procederá a resolver los supuestos prácticos y/o preguntas puestos a su disposición para cada tema. Ello exige como presupuesto irrenunciable, la lectura previa detenida de cada tema. La realización de dichos ejercicios provee al alumno/a de una serie de ventajas:

a) Por un lado, acompasa su ritmo de trabajo al considerado más adecuado por el Profesor para la preparación de la asignatura a través de la periodificación que marca el cronograma, pues la resolución de los supuestos prácticos exige la previa preparación y comprensión del tema correspondiente.

b) Asegura un conocimiento y entendimiento más sólido y duradero de los contenidos de la asignatura, se familiariza con una herramientas de estudio y de trabajo (técnicas a distancia, por medio de las TIC), que con toda seguridad serán empleadas cada vez más en la vida académica y profesional.

c) Permite al alumno/a valorar mejor las competencias adquiridas en relación directa con el esfuerzo realizado.

Por consiguiente, el alumno/a que no esté en condiciones o interesado/a en seguir esta forma de estudio y de (auto)evaluación no podrá asegurarse la adquisición de las competencias previstas para esta asignatura.

8. CRONOGRAMA

El cronograma o periodificación del trabajo para el seguimiento de la asignatura, es un instrumento complementario pero esencial para poder culminar con éxito la misma. En efecto, es un factor clave para organizar el estudio de cada tema, la realización sucesiva de las actividades aplicativas relacionadas con cada tema, la subsiguiente autoevaluación del estudio de cada tema y la actividad aplicativa correspondiente, y el trabajo final.

Dado que cada alumno puede tener circunstancias personales, laborales o de estudio (presencial u otro) diferentes, se presenta una propuesta de cronograma que puede adaptarse a cada situación. La duración del curso se establece para un período de cuatro meses (quince semanas). Para quien disponga de más tiempo o sea más impaciente puede concentrarla en dos meses (ocho semanas).

La primera variante, que nos parece más recomendable, en especial para todos aquellos que carezcan de implicaciones previas en la materia, comporta fijar siete períodos de dos semanas cada uno, durante el cual el alumno/a deberá realizar el estudio de un tema (7 temas en total), la actividad aplicativa correspondiente a ese mismo tema, y la autoevaluación del estudio y de la actividad. Y así sucesivamente. La última semana restante se dedicará a la redacción del trabajo final.

La segunda variante supone reducir a la mitad los plazos anteriores: cada semana un tema, y la última el trabajo final.

El alumno/a puede establecer un cronograma propio de similar estructura que se adapte mejor a sus necesidades y posibilidades. En este caso, debería fijarlo previamente al inicio del curso, y una vez decidido debería respetarlo con rigor.