Proyecto sobre la ciberdelincuencia
www.coe.int/cybercrime

y la

Red de Lisboa
www.coe.int/lisbon-network

Departamento de la Sociedad de Información y de Acción contra la Delincuencia
Dirección General de Derechos Humanos y Asuntos Jurídicos
Estrasburgo (Francia)

8 de octubre de 2009

Formación en delincuencia para jueces y fiscales: una idea

Proyecto financiado por contribuciones provenientes de Rumania, Microsoft y MacAfee, y por el Consejo de Europa

El presente documento ha sido elaborado por un grupo de trabajo integrado por múltiples partes interesadas en el marco del Proyecto sobre la ciberdelincuencia y la Red de Lisboa de instituciones de formación judicial del Consejo de Europa.

Dirección de contacto:

Para más información, diríjase a:

Departamento de la Sociedad de Información y de Acción contra la Delincuencia
Dirección General de Derechos Humanos y Asuntos Jurídicos
Consejo de Europa
Estrasburgo (Francia)

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Correo electrónico: alexander.seger@coe.int

Índice

1 Resumen ejecutivo

Dada la dependencia de las sociedades del mundo respecto de las tecnologías de la información y la comunicación, los jueces y fiscales deben estar preparados para ocuparse de la ciberdelincuencia y las pruebas electrónicas. Si bien en muchos países las fuerzas del orden han podido reforzar su capacidad para investigar ciberdelitos y obtener pruebas electrónicas, al parecer esto no ha sido tanto así en el caso de jueces y fiscales. La experiencia demuestra que, en muchos casos, estos últimos tienen dificultades para adaptarse a las nuevas realidades del ciberespacio. Por consiguiente, es preciso desplegar esfuerzos especiales para que los jueces y fiscales puedan procesar a ciberdelincuentes y tengan las competencias para juzgarlos y utilizar pruebas electrónicas, gracias a la formación, la colaboración en red y la especialización.

La presente idea consiste en ayudar a desplegar tales esfuerzos. La idea ha sido desarrollada a lo largo de 2009 por el Proyecto sobre la ciberdelincuencia y la Red de Lisboa de instituciones de formación judicial del Consejo de Europa, con la cooperación de un grupo de trabajo multipartito.

Así pues, la finalidad es ayudar a las instituciones de formación judicial a elaborar programas de formación sobre ciberdelincuencia y pruebas electrónicas para jueces y fiscales e integrar dichos programas en la formación inicial y en el empleo (es decir, institucionalizarla). Otro objetivo es facilitar la colaboración en red de jueces y fiscales con el fin de mejorar sus conocimientos sobre estos temas y prestar asistencia sistemática – en lugar de circunstancial – a las iniciativas de formación que prestan los asociados interesados.
La idea consta de los siguientes elementos:

Objetivos

Por lo general, la formación inicial y en el empleo actuales no proporcionan a los jueces y fiscales el nivel de conocimientos necesario para tratar la ciberdelincuencia y las pruebas electrónicas.

Por ese motivo, la idea de formar a jueces y fiscales tiene por objetivos:

- Permitir a las instituciones de formación jurídica impartir formación inicial y en el empleo sobre ciberdelincuencia, con arreglo a las normas internacionales
- Dotar al mayor número posible de jueces y fiscales en activo y futuros con los conocimientos básicos en materia de ciberdelincuencia y pruebas electrónicas
- Impartir formación avanzada a un número adecuado de jueces y fiscales
- Fomentar la especialización y la formación técnica continuas de jueces y fiscales
- Contribuir a mejorar los conocimientos mediante la colaboración en red de jueces y fiscales
- Facilitar el acceso a las diferentes redes e iniciativas de formación.

Las siguientes medidas deberían ayudar a alcanzar estos objetivos:

1. Institucionalización de la formación inicial

- En los países donde la formación inicial comprenda unas prácticas en el empleo, se recomienda que al menos una parte de dicha formación se dedique a la ciberdelincuencia y a los delitos electrónicos
- En los países donde la formación inicial se imparte en instituciones de formación judicial, el programa de estudios debería incluir como mínimo un módulo de nivel básico sobre ciberdelincuencia y delitos electrónicos. Además, estos temas deben tratarse en los módulos obligatorios relativos al derecho sustantivo y derecho procesal. También deben ofrecerse módulos facultativos de nivel avanzado sobre ciberdelincuencia y delitos electrónicos
- Los módulos de formación específica deben estar normalizados para que sean reproducibles y permitan a los candidatos pasar del nivel básico al avanzado.

2. Institucionalización de la formación en el empleo

- Las instituciones de formación en el empleo deberían ofrecer al menos un módulo de nivel básico sobre ciberdelincuencia y pruebas electrónicas para que los jueces y fiscales puedan adquirir los conocimientos básicos que no obtuvieron durante su formación inicial
- También deberían ofrecer cursos de nivel avanzado.

3. Cursos/módulos normalizados y reproducibles

- Deberían prepararse cursos o módulos que puedan reproducirse a gran escala de manera rentable y que permitan a los jueces y fiscales candidatos y en activo pasar del nivel básico al avanzado
- Deberían evaluarse los cursos básicos existentes para determinar si pueden integrarse en el programa de estudios de la formación inicial o en el empleo. Luego se podría recomendar un curso estándar a las instituciones que ofrecen formación inicial o en el empleo
- Podría realizarse una evaluación similar de los cursos de nivel avanzado, para luego recomendar un curso avanzado estándar
- Podría ser necesario formar instructores locales para dichos cursos a fin de que sean ellos quienes los impartan en el idioma local y recurrir lo menos posible a instructores internacionales.

4. Acceso a material didáctico o autodidáctico

- Debería prepararse material didáctico que responda a las normas internacionales comunes y a las prácticas idóneas, y ponerlo a disposición de las instituciones docentes a buen precio para que pueda utilizarse a escala local.
- Aunque los jueces y fiscales han de recibir formación principalmente para la aplicación de la legislación nacional, es posible crear material didáctico normalizado que sea lo suficientemente general para tener en cuenta la legislación y los sistemas nacionales.
- Se deberían preparar y ofrecer cursos en línea.

5. Centros piloto para la formación básica y avanzada

- Deberían crearse varios centros piloto para la formación básica y avanzada de jueces y fiscales en materia de ciberdelincuencia y pruebas electrónicas, a los efectos de probar y mejorar cursos y material didáctico normalizado, divulgar prácticas óptimas, realizar investigación sobre formación, mantener un registro de instructores e impartir formación a otros países con sistemas e idiomas similares
- Los centros piloto deberían coordinar sus actividades entre sí, con la asistencia del Consejo de Europa
- Los jueces y fiscales que deseen convertirse en expertos deben considerar la posibilidad de participar en la formación que ofrezcan los centros de excelencia a las fuerzas del orden y al sector privado.

6. Mejorar los conocimientos mediante la colaboración en red

- Además de la formación, también será esencial la cooperación y la colaboración en red entre jueces y fiscales, así como con otros interesados
- Jueces y fiscales deberían utilizar las redes de jueces y fiscales existentes (tales como la red GPEN)
- El Consejo de Europa debería considerar la posibilidad de crear una red internacional de jueces especializados en ciberdelincuencia y delitos electrónicos (similar a la red GPEN para fiscales)

- El Consejo de Europa y la Red Europea de Formación Judicial deberían fomentar la colaboración en red de las instituciones europeas que ofrecen formación sobre ciberdelincuencia y pruebas electrónicas
- Para facilitar a los jueces y fiscales el acceso a éstas y otras muchas redes relacionadas con la ciberdelincuencia, el Consejo de Europa debería elaborar un registro de iniciativas y redes, y crear un portal con enlaces, información sucinta e información de contacto acerca de las distintas redes. Este portal facilitará, además, la coordinación entre las redes y el acceso a las iniciativas y al material didáctico existente.

7. Cooperación entre los sectores público y privado

- La colaboración del sector privado en la formación de jueces y fiscales sería útil, por cuanto el sector privado dispone de gran experiencia sobre este particular. Por otra parte, debe mantenerse la independencia e imparcialidad de los jueces y fiscales
- Las instituciones de formación judicial pueden aprovechar la experiencia del sector privado al concebir programas de formación, preparar material didáctico e impartir cursos
- La colaboración del sector privado con las instituciones docentes no debe aprovecharse para obtener posibles decisiones favorables en los tribunales o hacer negocio, sino para garantizar que los jueces y fiscales reciben la información adecuada que les permita tomar decisiones con conocimiento de causa
- El sector privado podría ayudar de manera transparente a organizaciones internacionales o nacionales, universidades, iniciativas de formación o a terceros que, a su vez, podrán colaborar con instituciones docentes independientes
- Si bien los jueces y fiscales deben disponer de conocimientos generales sobre Internet y ciberdelincuencia, también es importante proporcionarles información relativa a plataformas específicas. El sector privado podría ofrecer material para módulos específicos (en lugar de cursos completos) sobre el funcionamiento de las principales plataformas.

La Red de Lisboa del Consejo de Europa aprobó esta idea en septiembre de 2009 y recomendó su divulgación general y su aplicación por parte de las instituciones de formación judicial. Por otra parte, decidió informar al respecto al Consejo Consultivo de Jueces Europeos y al Consejo Consultivo de Fiscales Europeos, así como a la Comisión Europea para la eficacia de la justicia (CEPEJ) con el fin de que esta idea reciba la mayor aceptación posible.

2 Introducción

En los últimos años las sociedades del mundo han registrado enormes progresos hacia su transformación en sociedades de la información. Las tecnologías de la información y la comunicación (TIC) están presentes en prácticamente todos los aspectos de la vida cotidiana. Debido a que las TIC se utilizan cada vez más y que, por tanto, existe una mayor dependencia respecto de las mismas, las sociedades son ahora vulnerables a amenazas tales como la ciberdelincuencia, es decir, los delitos que se cometen contra un sistema informático o sus datos, o utilizando dichos sistemas.

Aparte de los numerosos delitos que se cometen contra las TIC o utilizando estas tecnologías, un número cada vez mayor de otros casos que llegan a los tribunales integran pruebas electrónicas almacenadas en sistemas informáticos u otros dispositivos.

Por consiguiente, los jueces y fiscales deben estar preparados para tratar el tema de la ciberdelincuencia y las pruebas electrónicas. Según declaró el Consejo Consultivo de Jueces Europeos[1], "es esencial que después de haber terminado todos los estudios de derecho, los jueces reciban formación detallada y diversa para que puedan desempeñar satisfactoriamente su cometido" (párrafo 3), "Dicha formación garantiza además su independencia e imparcialidad" (párrafo 4), y en la formación se debe "tomar en consideración la necesidad de conciencia social y grandes conocimientos de los diferentes temas que muestran la complejidad de la vida en sociedad" (párrafo 27). Las TIC son tan importantes en las sociedades modernas que los jueces y fiscales deben de disponer al menos de un nivel de conocimientos básico de tales tecnologías y los problemas que entrañan.

Si bien en muchos países las fuerzas del orden han podido reforzar su capacidad para investigar ciberdelitos y obtener pruebas electrónicas, al parecer esto no ha sido tanto así en el caso de jueces y fiscales, quienes no obstante desempeñan un papel esencial en el proceso de enjuiciamiento criminal. La experiencia demuestra que, en muchos casos, los jueces y fiscales tienen dificultades para adaptarse a las nuevas realidades del ciberespacio.

Por consiguiente, es preciso desplegar esfuerzos especiales para que los jueces y fiscales puedan procesar a ciberdelincuentes y tengan las competencias para juzgarlos y utilizar pruebas electrónicas, gracias a la formación, la creación de redes y la especialización.

La experiencia del sector privado en materia de nuevas tecnologías ha resultado esencial para la formación de las fuerzas del orden. También será útil para la formación de jueces[2], pero hasta ahora esta posibilidad se ha desaprovechado. Por otra parte, debe mantenerse la independencia e imparcialidad de los jueces y fiscales. Así pues, se necesitan métodos innovadores para garantizar la independencia de jueces y fiscales y, al mismo tiempo, permitirles el acceso a la experiencia del sector privado y ayudarles a comprender el funcionamiento de la tecnología y la industria de las TIC. La idea que se propone en el presente documento muestra cómo las instituciones de formación judicial pueden beneficiarse de la ayuda del sector privado y la universidad a través de programas de formación normalizados y otros mecanismos.

La finalidad de la idea presentada en este informe es ayudar a las instituciones docentes de jueces a preparar programas de formación sobre ciberdelincuencia y pruebas electrónicas destinados a jueces y fiscales, e integrar dichos programas en la formación inicial y en el empleo (es decir, institucionalizarla).

---

[1] Opinión Nº 4 sobre la adecuada formación inicial y en el empleo de jueces a los niveles nacional y europeo (CCJE (2003) Op. Nº 4)

[2] Véase el estudio publicado en marzo de 2009: "Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel"

La idea se basa en la información recibida de instituciones docentes de Bélgica, Croacia, Georgia, Alemania, Francia, Países Bajos, Polonia, Portugal, Rumania, España, "la ex República Yugoslava de Macedonia" y el Reino Unido (respuestas al cuestionario recibidas al mes de junio de 2009), el taller celebrado en Portugal el mes de julio de 2009 al que asistieron representantes de Bélgica, Irlanda, Italia, Portugal, Países Bajos y Reino Unido, así como del sector privado, y el taller celebrado en Estrasburgo los días 3 y 4 de septiembre de 2009, en el que participaron representantes de instituciones docentes, jueces y fiscales de los países mencionados, del sector privado y de la Red Europea de Formación de Jueces y de la Red de Lisboa del Consejo de Europa.[3]

Este proceso multipartito dio lugar a la elaboración, por vez primera, de una idea para la formación de jueces y fiscales en materia de ciberdelincuencia y pruebas electrónicas. Habida cuenta de la naturaleza participativa de este proceso, no cabe duda de que la puesta en práctica de esta idea facilitará la cooperación entre las distintas partes interesadas y la convergencia de conocimientos y experiencia.

La Red de Lisboa del Consejo de Europa aprobó esta idea en septiembre de 2009 y recomendó su divulgación general y su aplicación por parte de las instituciones de formación judicial. Asimismo, decidió informar al respecto al Consejo Consultivo de Jueces Europeos, al Consejo Consultivo de Fiscales Europeos y a la Comisión Europea para la eficacia de la justicia (CEPEJ) con el fin de que esta idea reciba la mayor aceptación posible.

[3] Red de Lisboa para el intercambio de información entre personas y entidades encargadas de la formación de jueces.

3 Instituciones[4] y sistemas de formación

En Europa – y otras regiones – los sistemas de formación de jueces y fiscales son muy diversos.[5]

En lo que respecta a la formación inicial, los sistemas suelen consistir en una combinación de lo siguiente[6]:

- Sistema A: una vez terminada la licenciatura en derecho y, a menudo, después de aprobar un examen de acceso, los candidatos reciben formación específica en un centro de formación judicial para convertirse en jueces y/o fiscales. Los jueces y fiscales reciben formación en una misma institución o a veces en instituciones diferentes.
- Sistema B: una vez terminada la licenciatura en derecho, los candidatos adquieren experiencia en el empleo (a veces en pasantías oficiales) en la Fiscalía, los tribunales, gabinetes de abogados u otras instituciones, antes de pasar un examen que los faculta a trabajar como abogados, fiscales y jueces. No intervienen instituciones de formación específica centralizadas.[7]

Formación en el empleo, es decir, formación profesional continua de jueces y fiscales en activo, que ofrecen bien las instituciones de formación judicial públicas que también son responsables de la formación inicial (por ejemplo, Francia, Georgia, Países Bajos, Polonia, Portugal, Rumania, España, "la ex República Yugoslava de Macedonia", Croacia), bien instituciones docentes creadas especialmente para la formación en el empleo (como en Alemania), o bien por otras instituciones públicas, organizaciones no gubernamentales, organizaciones internacionales o el sector privado. En algunos casos esta formación se ofrece en el marco de los planes anuales de formación o bien se imparte *ad hoc*. En muchos casos, la formación en el empleo es facultativa, salvo para los jueces o fiscales que ejercen sus funciones en tribunales especializados (por ejemplo, en Rumania).

[4] A los efectos del presente documento, por institución de formación se entiende toda entidad encargada de impartir formación.

[5] Según declaró en 2003 el Consejo Consultivo de Jueces del Consejo de Europa en 2003: "Existe una gran diversidad entre los diferentes países de Europa, en cuanto a la formación y al desarrollo profesional de los jueces. Dichas diferencias pueden estar, en parte, relacionadas con las características particulares de los distintos sistemas judiciales, pero en algunos aspectos no parecen ser inevitables o necesarias. Algunos países proponen una formación institucionalizada de larga duración impartida en un centro especializado y seguida de una formación continua intensiva. Otros prevén una especie de aprendizaje bajo la tutela de un juez experimentado, que imparta conocimientos y consejos profesionales sobre ejemplos concretos, mostrando la marcha a seguir y evitando cualquier tipo de didactismo. Los países de la *Common law* dan una gran importancia a una larga experiencia profesional, habitualmente como abogados. Entre dichas posibilidades existe toda una variedad de países en los que la formación está más o menos organizada y es más o menos obligatoria."
Opinión Nº 4 del Consejo Consultivo de Jueces Europeos (CCJE) a la atención del Comité de Ministros del Consejo de Europa sobre la formación inicial y continuada de los jueces a los niveles nacional y europeo (CCJE (2003) Op. N° 4; noviembre de 2003).

[6] Para mayor información, véase el anexo.

[7] Cabe mencionar las características específicas de los sistemas de la *common law*. En el Reino Unido, por ejemplo, los jueces se nombran de entre los abogados con experiencia. Los abogados que no ejercen como jueces a tiempo completo también tienen la posibilidad de ejercer a tiempo parcial al menos un mes al año, después de lo cual la gran mayoría se nombra como jueces a tiempo completo. Además, muchos se nombran a tiempo parcial para ejercer en Tribunales (civiles) y Tribunales de Magistrados (principalmente penales). Existen programas de formación antes de cada investidura y durante el ejercicio de sus funciones.

El programa de estudios para la formación inicial y en el empleo exige en muchos casos un examen oficial y un proceso de aprobación, aunque hay más flexibilidad en lo que respecta a la formación facultativa y en el empleo. Por ejemplo:

- En Francia los programas de estudios se crea a través de un proceso de consulta entre el poder judicial, los profesionales del derecho y los departamentos del Ministerio de Justicia, y luego se someten a la aprobación de la Junta Directiva de la Escuela.
- En Alemania, la Conferencia de Programas de la Escuela Judicial Alemana – integrada por representantes de las diferentes administraciones de sistemas de justicia y asociaciones profesionales de jueces y fiscales – se encarga de preparar el programa de estudios de la Escuela para la formación en el empleo.
- En Polonia, los departamentos del Ministerio de Justicia, los presidentes de los tribunales y la Fiscalía presentan propuestas antes del 30 de abril de cada año. Basándose en esas propuestas, el Director de la escuela nacional somete a la aprobación de la Junta de Programas el programa de actividades docentes para el siguiente año antes del 30 de julio. Una vez aprobado por el Ministerio de Justicia, el programa de formación se envía a los correspondientes departamentos del Ministerio de Justicia, a los presidentes de los tribunales de apelación y a los fiscales generales de los tribunales de apelación.
- En Rumania, la estrategia para la formación inicial y en el empleo la aprueban el Consejo Científico del Instituto Nacional de Magistrados y el Consejo Superior de la Magistratura.
- En España, los planes de estudio y los programas de formación los prepara una Comisión pedagógica constituida por expertos en asuntos jurídicos, en consulta con asociaciones de jueces y jueces independientes. Los programas de estudios de la formación inicial y en el empleo para jueces los aprueba luego el Consejo General del Poder Judicial.
- En Portugal, el Centro de Estudios Judiciales prepara cada año un programa de formación. Aunque el programa de estudios de la formación inicial queda definido por ley, el programa de formación en el empleo se cambia cada año en función de las necesidades identificadas en la práctica. El programa de formación se crea tras consultar al Consejo Superior del Poder Judicial, a los tribunales fiscales y administrativos y a la Fiscalía.
- En Bélgica, el « Institut de formation judiciaire » prepara o supervisa cada año los programas de formación general o más específica. Este Instituto fue creado recientemente por ley (31/01/07) y comenzó sus actividades a principios de 2009. La ciberdelincuencia puede incluirse en la formación en el empleo (a menudo opcional).
- El los Países Bajos, el Consejo de Jueces y el Consejo de Fiscales Generales (que juntos dan instrucciones al Centro de formación judicial, el SSR) deciden si hay o no presupuesto para la formación propuesta. Por ejemplo, pueden formular propuestas los fiscales, los jueces o los instructores del SSR y, si hay presupuesto y se aprueban, el programa de formación lo elaboran los correspondientes expertos del SSR, el servicio de la fiscalía, los jueces y, si procede, terceros, incluidos el sector privado.
- En Croacia, el programa de estudios de la formación inicial y los planes de formación en el empleo se crean en cooperación con el Consejo Asesor y el Consejo de Programas de la Escuela Judicial. El Consejo de Programación determina las prioridades de formación y presenta la propuesta para el proyecto de programa de estudios anual de la formación profesional. El Consejo Asesor adopta el documento y establece las pautas para definir la estrategia de la formación profesional. Los Miembros de los dos Consejos son expertos jurídicos de renombre y representantes de todos los grupos de la Escuela Judicial.

Las instituciones de formación pueden recurrir a expertos externos, especialmente si los temas son muy específicos y técnicos, como es el caso de la ciberdelincuencia y las pruebas electrónicas. Por ejemplo:

- En Alemania, la Escuela Judicial Alemana recurre sobremanera a profesores externos, en su mayoría profesionales o investigadores del derecho, aunque a veces pueden ser expertos de la industria.

- En Países Bajos, consultores y expertos de la industria participan en la preparación de cursos de formación e imparten dichos cursos.
- En Rumania, el Instituto Nacional de Magistrados recurre a profesores e instructores externos en campos especializados tales como la ciberdelincuencia (por ejemplo, el Consejo de Europa, el Departamento de Justicia de Estados Unidos, el FBI, el Servicio Secreto de Estados Unidos y entidades del sector privado, tales como eBay, Visa, American Express, Amazon, PayPal, Microsoft), en particular, para la formación de instructores.
- En España, el Consejo General del Poder Judicial ha firmado acuerdos con empresas del sector privado (CYBEX, Logality) para impartir formación sobre ciberdelincuencia e informática forense. Expertos del sector privado participan en la formación judicial.
- En Portugal, la mayoría de los instructores del Centro de Estudios Judiciales son jueces o fiscales. En la formación en el empleo (por ejemplo, seminarios o cursos breves) pueden participar instructores y otros expertos del sector privado.
- En Croacia, especialistas de la policía especializada en la lucha contra el crimen organizado y los delitos económicos participan en la elaboración y suministro de formación.
- En Bélgica, las universidades administran una buena parte del presupuesto que se destina a la formación de jueces y fiscales. No obstante, en algunos programas de formación pueden participar expertos del sector privado.

Las repercusiones para la formación de jueces y fiscales en materia de ciberdelincuencia/pruebas electrónicas son las siguientes:

- Por regla general, los jueces y fiscales comienzan su formación en la universidad con los estudios de derecho. Puede suponerse que cuanta más legislación haya sobre cuestiones relativas a la ciberdelincuencia y las pruebas electrónicas, más se tratarán estos temas en los libros de texto y el programa de estudios de derecho. Ahora bien, convendría formular propuestas a este respecto a los responsables de preparar el material didáctico para los estudios universitarios.
- En países donde la formación inicial se lleva a cabo en instituciones de formación judicial, debería ser posible incluir el tema de la ciberdelincuencia/pruebas electrónicas en el plan de estudios.
- Esto es más difícil cuando la formación inicial se realiza en el empleo.
- En muchos países, hay instituciones de formación judicial que ofrecen formación en el empleo, por lo que debería ser posible integrar los temas de ciberdelincuencia/pruebas electrónicas en el programa de estudios.
- Si bien es posible ofrecer formación en el empleo *ad hoc*, para incluir la formación sobre ciberdelincuencia /pruebas electrónicas en el programa oficial de estudios se han de seguir los procedimientos de aprobación oficiales, es decir, institucionalizar dicha formación.
- La formación en el empleo suele ser facultativo, por lo que el problema radicará en convencer a jueces y fiscales de que cursen la formación en una campo técnico como el de la ciberdelincuencia /pruebas electrónicas.[8]
- Se necesita recurrir a los conocimientos de expertos externos de los sectores público y privado para preparar los cursos de formación, formar a instructores e impartir dichos cursos.

[8] En Portugal, la formación en el empleo es obligatoria (es decir, cada juez y fiscal debe asistir, como mínimo, a dos eventos de formación al año), mientras que en Rumania puede ser obligatoria en algunos casos.

4 Competencias y conocimientos que deben tener los jueces y fiscales

Es evidente que cada vez llegarán a los tribunales, tanto penales como civiles y administrativos, un mayor número de delitos que de un modo u otro guardan relación con las tecnologías de la información y la comunicación, y que la mayoría de los jueces y fiscales tendrán que ocuparse de casos de ciberdelincuencia o, al menos, de casos en los que se aportan pruebas electrónicas. Por consiguiente, no basta con formar solamente a jueces y fiscales especializados.

Es indispensable una gran divulgación de conocimientos en materia de ciberdelincuencia y pruebas electrónicas: todos los jueces y fiscales o, el mayor número posible de ellos, deberán recibir como mínimo formación básica sobre ciberdelincuencia y pruebas electrónicas. Estos conocimientos básicos deberían adquirirse durante la formación inicial de futuros jueces y fiscales y en el marco de la formación en el empleo de jueces y fiscales en activo.

Al mismo tiempo, estas cuestiones son muy técnicas y evolucionan constantemente, por lo que no cabe esperar que los jueces y fiscales en general puedan mantenerse al corriente de los últimos adelantos tecnológicos en todo momento. Por consiguiente, es necesario que un número suficiente de jueces y fiscales reciban conocimientos avanzados para que se conviertan en especialistas en ciberdelincuencia y pruebas electrónicas.

4.1 Conocimientos básicos

En la mayoría de los sistemas judiciales no puede saberse de antemano qué juez se encargará de un determinado caso (principio del derecho natural) por lo que, en última instancia, todos los jueces, jueces de instrucción y fiscales deben tener conocimientos básicos de asuntos relacionados con la ciberdelincuencia y las pruebas electrónicas. Por "conocimientos básicos" se entiende que deben ser capaces de comprender lo siguiente:

- Ordenadores y redes: cómo funcionan, nociones básicas del funcionamiento de Internet, la función de los proveedores de servicio, problemas particulares a los que se enfrentan jueces y fiscales
- Ciberdelincuencia: cómo se utilizan las tecnologías de la información y la comunicación para cometer delitos
- Legislación sobre ciberdelincuencia: legislación nacional (comprendida la jurisprudencia) y normas internacionales
- Jurisdicción y competencias territoriales
- Pruebas electrónicas: procedimientos técnicos y aspectos jurídicos.

Tras recibir este tipo de formación básica, los jueces y fiscales deberían ser capaces de:

- Relacionar los actos delictivos con las correspondientes disposiciones de la legislación nacional
- Aprobar técnicas de investigación
- Ordenar la búsqueda y confiscación de sistemas informáticos y la obtención de pruebas electrónicas
- Acelerar la cooperación internacional
- Interrogar a testigos y expertos
- Presentar/validar pruebas electrónicas.

A continuación se muestra un ejemplo de curso de formación básica característico para jueces y fiscales.

Ejemplo: Formación en ciberdelincuencia y pruebas electrónicas – módulo de nivel básico

Objetivo del curso	Al final del curso los jueces y fiscales dispondrán de los conocimientos básicos acerca de la ciberdelincuencia y las pruebas electrónicas, la forma de tratar estos asuntos, el derecho sustantivo y procesal y las tecnologías que pueden emplearse, así como la forma de adoptar medidas urgentes y eficientes y de lograr una amplia cooperación internacional
Sesión 1	Acerca de la ciberdelincuencia
	• ¿Por qué preocuparse de la ciberdelincuencia? • ¿Qué es la ciberdelincuencia? • Problemas que plantea a jueces y fiscales • Legislación nacional y normas internacionales
Sesión 2	Tecnología
	• Funcionamiento de Internet (nociones básicas) • Glosario de términos • Protocolos
Sesión 3	La ciberdelincuencia contemplada como delito en la legislación nacional
	• Delitos contra los sistemas informáticos y de datos • Fraude y falsificación informáticos • Delitos relacionados con el contenido (pornografía infantil, xenofobia, racismo) • Delitos relacionados con la propiedad intelectual • Decisiones judiciales/derecho jurisprudencial
Sesión 4	Pruebas electrónicas
	• Pruebas electrónicas: definiciones y características • Requisitos de las pruebas electrónicas • Informática forense
Sesión 5	Derecho procesal/diligencias para la instrucción del proceso
	• Jurisdicción y competencias territoriales • Protección acelerada de datos informáticos • Dictado de sentencias/autos • Búsqueda y obtención de datos informáticos • Intercepción de tráfico y de datos de contenido • Salvaguardas
Sesión 6	Relaciones con el sector privado
Sesión 7	Cooperación internacional
	• El Convenio sobre la ciberdelincuencia como marco para la cooperación internacional • Principios generales • Medidas provisionales y la función de los servicios de contacto 24/7 • Asistencia jurídica mutua y función de las autoridades competentes
Sesión 8	Evaluación y conclusión
Logística y materiales	La formación podrá ofrecerse en línea o en un aula. Si se imparte en un aula: • Un aula equipada con un PC y un proyector para las ponencias es suficiente (dado que en este curso no se hacen ejercicios prácticos, tales como demostración de programas de informática forense o técnicas de investigación, tampoco se necesita un laboratorio de informática) • Extractos pertinentes del derecho sustantivo y del derecho procesal nacionales • Convenio de Budapest sobre la ciberdelincuencia y su informe explicativo • Libro de texto con glosario de términos y otra información de referencia

- Si las clases se imparten en un idioma extranjero, debe preverse un servicio de interpretación y la traducción del material.

4.2 Conocimientos avanzados

A veces no basta con disponer de los conocimientos básicos para ocuparse de un caso de ciberdelincuencia. Para afrontar este tipo de situaciones, será necesario que un número considerable de jueces, jueces de instrucción y fiscales tengan conocimientos avanzados para poder investigar, procesar, y juzgar casos complejos relacionados con la ciberdelincuencia y las pruebas electrónicas, o para prestar ayuda a otros fiscales y jueces.

En algunos países se han creado unidades o departamentos especializados en estos temas (por ejemplo, Rumania, Serbia), mientras que en otros la fiscalía dispone de varios fiscales especializados. En los Países Bajos se creó el programa "intensiveringsprogramma" para garantizar, entre otras cosas, que haya al menos un fiscal especializado en ciberdelincuencia en cada una de las once oficinas más grandes de la fiscalía. En Italia, en virtud de la nueva legislación sobre ciberdelincuencia, 29 oficinas de la fiscalía disponen ahora de jurisdicción en asuntos relacionados con la ciberdelincuencia. En Portugal, la fiscalía del distrito de Lisboa cuenta con una sección especializada en delitos informáticos, a la que se remiten este tipo de investigaciones.

En algunos países, ciertos fiscales pueden supervisar el trabajo de unidades de la policía especializadas en delitos de alta tecnología. En la mayoría de los países, la fiscalía tiene una estructura jerárquica de forma que el fiscal superior pueda asignar el caso a un fiscal especializado. Así pues, es posible identificar los fiscales que deben tener un nivel avanzado de conocimientos en esta materia.

En lo que respecta a los jueces, en algunos países es posible asignar los casos de ciberdelincuencia a jueces especializados de un tribunal que se encarga de determinados tipos de delitos, por ejemplo del crimen organizado. Como ejemplo (posiblemente el único de Europa) puede citarse a Serbia, donde el departamento especial del tribunal del distrito de Belgrado se encarga de los casos de ciberdelincuencia. Ahora bien, habida cuenta del principio de derecho natural que se aplica en la mayoría de los sistemas judiciales, es necesario adoptar un método diferente. En los Países Bajos, quizá el único país en Europa, se han creado cinco centros con jueces especializados que actúan de asistentes de otros jueces. En España, el Consejo General del Poder Judicial está estudiando una propuesta similar en la que un grupo de jueces especializados en ciberdelincuencia y pruebas electrónicas prestaría asistencia y asesoramiento a otros jueces. En Bélgica, la legislación no exige especialización alguna, pero la mayoría de los tribunales tienen la posibilidad de exigir a uno o varios de sus miembros que se especialicen. Huelga decir que la atribución de este tipo de casos a los jueces especializados es sólo una cuestión de organización interna del tribunal. En algunas ocasiones, la legislación estipula la competencia para juzgar ciertos casos a determinados tribunales del país (Bruselas). Sin embargo, en la mayoría de los casos la competencia queda determinada por el lugar donde se comete el delito y el juez/fiscal especializado no siempre se encuentra allí. En muchos países ciertos tribunales se ocupan de casos de ciberdelincuencia con más frecuencia que otros, por lo que requieren un nivel más alto de especialización que los demás.

Por "conocimientos avanzados" se entiende que los jueces y fiscales comprenden los aspectos prácticos y son capaces de aplicar sus conocimientos a lo siguiente:

- Ordenadores y redes:
  - Glosario de términos informáticos y de ciberdelincuencia
  - Funcionamiento de Internet
  - Protocolos y tecnología

- Función de los proveedores de servicio

- Ciberdelincuencia:
  - Tendencias en la ciberdelincuencia
  - Tipologías: Tipos particulares y técnicas de ciberdelincuencia (por ejemplo, *peska* (*phishing*), redes robot y otro software malicioso, pornografía infantil)
  - Ejemplos prácticos y simulaciones

- Legislación sobre ciberdelincuencia:
  - Legislación nacional y jurisprudencia
  - Cooperación internacional: acuerdos internacionales y bilaterales, canales de cooperación judicial y mecanismos prácticos para la cooperación acelerada

- Investigación y pruebas electrónicas:
  - Jurisdicción y competencias territoriales
  - Disposiciones del derecho procesal y su aplicación práctica
  - Fases de la investigación, obtención y conservación de pruebas electrónicas
  - Características de los programas de informática forense
  - Identificación de sospechosos
  - Rastreo del dinero ilícito
  - Salvaguardas y condiciones
  - Presentación de pruebas electrónicas en los tribunales.

Ejemplo: formación en ciberdelincuencia y pruebas electrónicas – módulo de nivel avanzado[9]

Objetivo del curso	Al final del curso los jueces y fiscales dispondrán de los conocimientos avanzados, que luego podrán poner en práctica, sobre el funcionamiento de ordenadores y redes, la ciberdelincuencia y la legislación al respecto, la jurisdicción, los mecanismos de investigación y las pruebas electrónicas, así como la cooperación internacional
Sesión 1	Ordenadores y redes
	• Glosario de términos de informática y ciberdelincuencia • Funcionamiento de la infraestructura de las TIC /Internet - Protocolos y tecnología - Cómo se comunican los ordenadores - Investigación IP y pruebas electrónicas –números y nombres de los ordenadores - Función de los proveedores de servicio • Información de Internet - Recopilación de información - Utilización de bases de datos (ocultas) de Internet • Características de grupos sociales - Formas de comunicación - Formas de lograr el anonimato • Detección/determinación de la ubicación y de la identidad de ordenadores, empresas y personas en Internet
Sesión 2	Ciberdelincuencia y riesgos de seguridad
	• Tendencias en la ciberdelincuencia • Tipologías: Tipos particulares y técnicas de ciberdelincuencia (por ejemplo, peska (phishing), redes robot y otro software malicioso, pornografía infantil) • Cómo utilizan los delincuentes las tecnologías de la información y la comunicación • Delincuentes

[9] Basado en las respuestas al cuestionario y el ejemplo facilitado por Países Bajos.

	• Repercusiones de la ciberdelincuencia • Cómo mejorar la seguridad de las TIC • Ejemplos prácticos y simulaciones
Sesión 3	Legislación sobre ciberdelincuencia: derecho penal sustantivo
	• Delitos contra los sistemas y datos informáticos • Fraude y falsificación informáticos • Delitos relacionados con el contenido (pornografía infantil, incitación de la violencia) • Delitos relacionados con la propiedad intelectual • Decisiones judiciales/jurisprudencia
Sesión 4	Investigación y pruebas electrónicas
	• Pruebas electrónicas - Rastros/huellas en computadores, Internet, comunicación digital - Fases para la investigación, obtención y conservación de pruebas electrónicas - Características de los programas de informática forense - Identificación de sospechosos - Rastreo del dinero ilícito - Salvaguardas y condiciones - Gestión/preparación de un caso - Presentación de pruebas electrónicas en los tribunales • Organización de la aplicación de la ley en el campo de la ciberdelincuencia/pruebas electrónicas • Estudios de caso
Sesión 5	Legislación sobre ciberdelincuencia: derecho procesal
	• Conservación acelerada de datos informáticos • Dictado de sentencias/autos • Búsqueda y obtención de datos informáticos • Intercepción de tráfico y de datos de contenido • Salvaguardas • Relaciones con los proveedores de servicios Internet y el sector privado • Estudios de caso
Sesión 6	Jurisdicción y competencias territoriales
	• Principios generales • Jurisdicción sobre ciberdelincuencia - problemas • Disposiciones relativas a la jurisdicción del Convenio sobre la ciberdelincuencia • Estudios de caso
Sesión 7	Cooperación internacional
	• El Convenio sobre la ciberdelincuencia como marco para la cooperación internacional • Principios generales • Medidas provisionales y la función de los servicios de contacto 24/7 • Asistencia jurídica mutua y función de las autoridades competentes • Estudios de caso
Sesión 8	Evaluación y conclusiones
Logística y materiales	La formación podrá ofrecerse en línea o en un aula. Si se imparte en un aula: • Un aula equipada con un PC y un proyector para las ponencias • Sería útil que los alumnos tuvieran un ordenador con acceso a Internet (pero no es imprescindible) • Extractos pertinentes del derecho sustantivo y del derecho procesal nacionales • Convenio de Budapest sobre la ciberdelincuencia y su informe explicativo • Libro de texto con un glosario de términos y otra información de referencia

- Si las clases se imparten en un idioma extranjero, debe preverse un servicio de interpretación y la traducción del material.

Por regla general, los jueces y fiscales no necesitan tener el mismo nivel de competencias y conocimientos técnicos que los investigadores de delitos de alta tecnología o de los informáticos forenses. Sin embargo, conviene recordar los esfuerzos desplegados hasta elaborar un programa de formación sistemático para los funcionarios de la fuerzas del orden público.

En el marco de un proyecto financiado por la Comisión Europea (Programa Falcone de 2002), dirigido por la policía irlandesa y con la participación de expertos de 10 Estados miembros de la UE, se elaboró un programa normalizado de formación básica sobre ciberdelincuencia ("Nivel 1") destinado a funcionarios de las fuerzas del orden. Desde 2004 se dispone de un curso de dos semanas que se ha impartido en muchos países de Europa y de otras regiones. El curso fue acreditado por University College Dublin (UCD) en 2006.

En el marco de otros proyectos dirigidos por la policía irlandesa en asociación con la UCD se prepararon módulos de niveles intermedio y avanzado con el objetivo general de crear un programa de licenciatura totalmente acreditado en informática forense e investigación de ciberdelincuencia, destinado a funcionarios de las fuerzas del orden. Los módulos de nivel intermedio para la aplicación de la ley son los siguientes:

- Investigación en Internet
- Investigación de redes
- Informática forense en NTFS
- Informática forense en Linux
- Análisis forense en telefonía móvil
- Redes LAN inalámbricas y VOIP
- Programación avanzada
- Análisis forense de datos en tiempo real
- Informática forense en Microsoft Vista.

Estos módulos se actualizan constantemente y se preparan módulos nuevos.[10]

En julio de 2007, Europol creó el Grupo para la armonización de la formación en investigación de ciberdelincuencia, destinado a coordinar en la UE las actividades de formación en delitos tecnológicos El principal objetivo es crear un programa de estudios certificado para investigadores de las fuerzas del orden de Europa y divulgar dicho programa en otras regiones con el fin de ayudar a los organismos de aplicación de la ley que desean ocuparse de estos asuntos. Entre los asociados se cuentan la Comisión Europea, OLAF, Eurojust, CEPOL, Interpol, Consejo de Europa, Naciones Unidas, Centro de investigación de ciberdelincuencia de UCD, Universidad de Troyes, Universidad Canterbury Christchurch, Universidad de Boloña, así como el sector privado.

4.3 Conocimientos especializados

Algunos jueces y fiscales pueden adquirir conocimientos especializados mediante estudios de postgrado, la autoformación, las redes dedicadas a estos temas o mediante la experiencia profesional. Dichos conocimientos no podrán formar parte de los programas de formación ordinarios. Los jueces y fiscales con dichos conocimientos especializados son muy útiles para los demás y para ejercer de instructores.

[10] Otros ejemplos son los programas sobre delincuencia de alta tecnología que ofrece la UK National Policing Improvement Agency.

5 Formación actual sobre ciberdelincuencia y pruebas electrónicas

5.1 Formación inicial

Por "formación inicial" se entiende la formación que reciben los candidatos – después de haber terminado los estudios superiores de derecho en la universidad – para poder convertirse en jueces y/o fiscales. En muchos sistemas, la formación inicial la imparte una institución de formación judicial durante un periodo de uno a tres años, mientras que en otros, dicha formación inicial consiste en pasantías más o menos oficiales sin un programa de estudios específico.

En la mayoría de los países, la ciberdelincuencia y las pruebas electrónicas no forman parte de la formación inicial o sólo en un grado muy limitado. Por ejemplo:

- En Francia, la formación de derecho procesal en la Ecole nationale de la magistrature (ENM) consta de una clase de tres horas que imparte un experto en TI sobre la búsqueda de pruebas electrónicas y sobre tecnología; no se tratan las cuestiones relativas a la ciberdelincuencia.
- En Georgia, estos temas no se estudian en la formación inicial de fiscales, pero en la de jueces y personal judicial se imparte un curso de medio día.
- En Alemania no se exigen estos temas en las pasantías.
- En Croacia, Polonia y Rumania estos temas no se incluyen en la formación inicial.

Ahora bien, en algunos países la ciberdelincuencia y las pruebas electrónicas son un tema ordinario en la formación inicial. Por ejemplo:

- En los Países Bajos, la formación inicial comprende un curso básico de un día sobre ciberdelincuencia que imparte el instituto de formación de jueces y fiscales (SSR) en Utrecht o Zutphen, en el que se distribuye un libro de texto y otro material de referencia. El curso consiste en seminarios interactivos y estudios de caso. Además de este curso básico de un día, se ofrece un curso intermedio de cuatro días y un curso avanzado de dos días.

- La Escuela Judicial de España ofrece formación inicial sobre ciberdelincuencia y pruebas electrónicas a jueces recién nombrados, tanto en derecho procesal como en cuestiones sustantivas, que forma parte de la formación obligatoria en derecho procesal y obtención de pruebas. Los temas de ciberdelincuencia y las pruebas electrónicas se tratan en seminarios que se imparte en cuatro tardes en los que se trata la legislación nacional, los instrumentos de cooperación internacional, los programas informáticos de análisis forense y de técnicas de investigación, la obtención de pruebas electrónicas y estudios de caso. Además, se organiza una vez al año un seminario especial sobre pruebas electrónicas y otro seminario sobre derecho sustantivo (delitos cometidos por medios electrónicos). Imparten estos seminarios expertos en temas jurídicos y en TI. Asimismo, los jueces tienen acceso a una biblioteca virtual sobre ciberdelincuencia. La finalidad de esta formación inicial es proporcionarles los conocimientos básicos sobre estos temas.

- En "la ex República Yugoslava de Macedonia", la Universidad de Formación de jueces y fiscales ofrece formación inicial sobre ciberdelincuencia y pruebas electrónicas como parte de la formación en derecho penal, en informática y en investigación. Se destinan diez horas a la ciberdelincuencia y las pruebas electrónicas.

- En Portugal la ciberdelincuencia no es un tema específico y autónomo del plan de estudios. Sin embargo, en el marco de la investigación criminal se imparte un seminario sobre ciberdelincuencia y pruebas digitales (de hora y media de duración). Durante la formación sobre derecho penal y derecho procesal, se destinan 9 horas a los delitos informáticos y medidas procesales para obtener pruebas digitales y 9 horas a las TIC.

Los cursos los imparten instructores permanentes, jueces, fiscales o abogados con experiencia en el tema, funcionarios de la policía especializados, expertos en informática o especialistas del sector privado.

De la información disponible se desprende que:

- Habida cuenta del objetivo de suministrar a jueces y fiscales un nivel básico de conocimientos en ciberdelincuencia y pruebas electrónicas, la formación que se ofrece es demasiado limitada.
- Con muy pocos excepciones, la formación inicial es de nivel básico y no se prevé la formación avanzada.
- Por lo general, no se dispone de un material de formación normalizado para que pueda reproducirse la formación.

5.2 Formación en el empleo

La formación en el empleo, es decir, la formación profesional continua de jueces y fiscales en activo, la ofrecen instituciones de formación judicial públicas y otros tipos de organizaciones. Por ejemplo:

- En Francia, la Ecole nationale de la magistrature organiza un seminario de nivel avanzado de cinco días de duración y ofrece además pasantías de dos días en la oficina central de delitos de alta tecnología del Ministerios del Interior (OLCTIC). La Escuela sufraga el coste del seminario (unos 5 000 euros por curso). Los instructores son jueces, fiscales, funcionarios de la policía, expertos en informática o expertos del sector privado.

- En Georgia, la Escuela Superior de Justicia es la única institución encargada de la formación en el empleo de jueces. Imparten un curso básico sobre ciberdelincuencia de dos días de duración, financiado con cargo al presupuesto del Estado. Los instructores son miembros de la facultad y jueces del Tribunal Supremo y de los tribunales de apelación. Los fiscales reciben formación del servicio de formación del Ministerio de Justicia, pero hasta la fecha aún no ofrecen cursos sobre ciberdelincuencia y pruebas electrónicas.

- En Alemania, la formación en el empleo de jueces y fiscales la imparte Deutsche Richterakademie que organiza unos 150 eventos al año. En 2009, dos de éstos trataron de la ciberdelincuencia, con una duración de cuatro días cada uno. Los instructores suelen ser fiscales y jueces con experiencia en cuestiones de ciberdelincuencia, pero algunos también proceden de la policía, las aduanas, las autoridades fiscales u otras. El coste se comparte entre el gobierno federal y el estatal. Estos cursos se ofrecen a nivel básico y avanzado.

- En Países Bajos, aunque la formación en el empleo es facultativa, cada juez está obligado a asistir un determinado número de horas de formación al año. El juez puede decidir a qué cursos asistir. El instituto de formación de jueces y fiscales (SSR), así como otras instituciones y centros de enseñanza de postgrado, ofrecen formación en el empleo sobre ciberdelincuencia y pruebas electrónicas de niveles básico y avanzado. La SSR ofrece cada año tres cursos de nivel básico y tres de nivel intermedio, y un curso avanzado. Los instructores son expertos en ciberdelincuencia de la fiscalía general y expertos del sector privado. Por otra parte, la SSR también ofrece una gran variedad de otros cursos de formación que tratan de los aspectos jurídicos y prácticos (en total a 400 cursos). Así pues, la ciberdelincuencia debe competir con todos estos cursos.

- En Polonia, la Escuela Nacional de jueces y fiscales ofrece cursos de niveles básico y avanzado, en la forma de conferencia con una duración de cuatro a cinco días. En 2009, se organizaron dos de esos eventos ("Metodología de delitos cometidos utilizando sistemas informáticos", "pruebas electrónicas en un juicio").

- En Rumania, el Instituto Nacional de Magistrados ofrece formación en el empleo pero sólo de nivel básico. Por ejemplo, entre 2006 y 2009, se organizaron cada año seminarios de dos días de duración, cada uno con la asistencia de 25 jueces/fiscales, financiados en su mayoría con el presupuesto del Instituto, algunos por la Comisión Europea (programa PHARE) y otros (en 2006) por eBay. Los instructores son magistrados rumanos, expertos en informática y expertos extranjeros financiados por organizaciones tales como el Consejo de Europa. Por otra parte, la ciberdelincuencia es un tema obligatorio de la formación descentralizada que se imparte en las oficinas de la fiscalía que dependen de tribunales de apelación. El Instituto coordina también esta formación.

- En España, la Escuela Judicial de España que dependen del Consejo General del Poder Judicial ofrece formación en el empleo a jueces sobre ciberdelincuencia y pruebas electrónicas. Para los fiscales, dicha formación la ofrece el Centro de Estudios Jurídicos que depende del Ministerio de Justicia. En ambos casos, la formación se organiza en cooperación con CYBEX, una empresa privada especializada en estos asuntos. La Escuela Judicial tiene un presupuesto de unos 42 000 euros para la formación en ciberdelincuencia. También es posible obtener financiación y asistencia del sector privado. Los cursos de formación en el empleo son de nivel básico, tienen una duración de tres a cuatro días, e incluyen teoría y análisis de casos prácticos. El material se publica y normalmente está al alcance de cualquier juez. En 2008 y 2009 se celebraron dos seminarios de este tipo al año. Si bien algunos asuntos se abordan con cierta profundidad, no existe un programa de formación sistemática de nivel avanzado.

- En Portugal, la formación en el empleo sobre ciberdelincuencia la imparte el Centro de Estudios Judiciales, que organiza unos 30 eventos al año. Dos de ellos tratan regularmente de cuestiones relativas a la ciberdelincuencia. A veces se ofrecen otros seminarios sobre asuntos conexos, tales como derecho de autor en línea o tecnología y los tribunales. Los instructores son jueces y fiscales, abogados, funcionarios de la policía y expertos de los sectores público y privado. Los seminarios tienen una buena acogida y cuentan con numerosos participantes (principalmente fiscales, pero también abogados y jueces de tribunales penales).

- En Bélgica el programa de formación en el empleo aún está en fase de desarrollo debido a la creación reciente del "Institut de formation judiciaire". La finalidad es, obviamente, organizar dicha formación teniendo presente los resultados y las recomendaciones de diversos grupos de expertos, en particular las observaciones formuladas por el Consejo de Europa. El Instituto puede financiar la participación de magistrados belgas en cursos en el extranjero a petición de éstos (por ejemplo, un juez y un fiscal asistieron a los cursos del Certificado Europeo de Cibercriminalidad y prueba electrónica organizado en París el mes de febrero de 2009).

- Actualmente, en Croacia no existe formación en el empleo sobre ciberdelincuencia y/o pruebas electrónicas. Este asunto se abordó únicamente en el marco del programa CARDS, en el que el país participó.

- En "la ex República Yugoslava de Macedonia" no se ofrece formación en el empleo.

- La Academia de Derecho Europeo (ERA) ofrece formación. ERA, creada oficialmente por iniciativa del Parlamento Europeo en 1992, tiene por objeto proporcionar conocimientos en profundidad y análisis del derecho Europeo y Comunitario, para lo cual organiza seminarios y cursos de orientación práctica para profesionales del derecho. La Academia es también un foro para el intercambio de experiencia y opiniones acerca del derecho europeo y las políticas. La ERA organiza regularmente eventos sobre ciberdelincuenia cuyos participantes proceden de toda la UE. En el periodo 2009-2010, ERA también está cooperando con TAIEX para impartir una serie de seminarios en Rumania, Bulgaria, los países candidatos y los posibles países candidatos, en los que se presentarán los principales instrumentos europeos e internacionales para luchar contra la ciberdelincuencia.

La finalidad de todos los seminarios es servir de plataforma para debatir y evaluar la forma en que se aplica la legislación europea sobre ciberdelincuencia en los diferentes Estados miembros y países candidatos, así como considerar la posibilidad de lanzar una campaña eficaz a nivel de toda Europa contra la utilización ilícita de Internet. Se debaten las leyes e instrumentos jurídicos más recientes de Europa, tales como el Convenio sobre la ciberdelincuencia del Consejo de Europa (2001), la Decisión Marco del Consejo 2005/222/JHA relativa a los ataques contra los sistemas de información y la Decisión Marco del Consejo 2004/68/JHA relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. También se aborda el tema de la cooperación en curso con los proveedores de servicios y sociedades web, como Google, Microsoft y Yahoo!.

En cada seminario se recurre de diversos métodos de formación, que varían desde clases de introducción y clases de nivel más avanzado, hasta estudios de casos y otros tipos de enseñanza interactiva. Se presta particular atención a las discusiones en pequeños grupos de trabajo. Las clases y los talleres los imparten expertos nacionales y de la UE.

- En varios países los eventos de formación se organizan en colaboración con el sector privado. Por ejemplo:

  En Alemania, eBay ha colaborado en el curso de formación sobre "nuevos medios y derecho penal" destinado a jueces y fiscales y organizado por la Deutsche Richterakademie, en el que participó un orador para presentar el portal de comercio electrónico de eBay, la actividad delictiva que suscita, las medidas existentes para combatir dicha actividad y la colaboración entre eBay y las fuerzas del orden. eBay también ha participado en varios cursos de formación 'puntuales' organizados por el Ministerio de Justicia de Berlín, a los que asistieron unos 100 fiscales cada vez.

  En Rumania, eBay ha organizado varios cursos de formación para jueces, fiscales y funcionarios de las fuerzas del orden. En particular, eBay colabora con el Servicio Secreto y la Embajada de Estados Unidos para formar a 25 fiscales de diferentes oficinas del DIICOT (Dirección para la investigación del crimen organizado y del terrorismo), 15 jueces y 20 funcionarios de la policía en Sibiu. Además, eBay partició en otros cursos de formación para jueces en Targu Jiu y otros 60 jueces de distintos tribunales que dependen del tribunal de apelación de Craiova.

Según se indicó antes, en prácticamente todos los casos, para modificar o ampliar el plan de estudios institucional sobre formación judicial se requerirá un proceso de aprobación y validación oficial.[11]

Aunque se han tomado muchas iniciativas para atender la necesidad de suministrar la formación adecuada sobre ciberdelincuencia a jueces y fiscales, es evidente que existe una falta de coherencia entre los métodos antes descritos.

[11] En este contexto, resulta interesante el proyecto de "Certificado Europeo sobre cibercibercriminalidad y prueba electrónica" ejecutado por CYBEX con fondos de la Comisión Europea (JPEN). El proyecto incluye un curso normalizado de nivel básico de cuatro días de duración destinado a jueces, fiscales y abogados. Entre principios de 2009 y finales de 2010 se probará el curso en 14 países piloto de Europa y América Latina. Los participantes recibirán un certificado que demuestra que han adquirido un nivel básico de conocimientos teóricos y prácticos, así como conocimientos jurídicos y técnicos sobre cuestiones relativas a las pruebas electrónicas y la ciberdelincuencia.
El Consejo de Europa también ha comenzado a preparar – en el marco del proyecto sobre ciberdelincuencia – un manual de formación para jueces y fiscales que se utilizará en un curso de nivel básico de dos días de duración consagrado a la legislación en materia de ciberdelincuencia.

Aun tomando en consideración las características específicas de cada legislación nacional y el hecho de que los sistemas educativos varían sobremanera, el problema de la ciberdelincuencia es, por las características que le son propias, de alcance internacional y, por ende, requiere un nivel mínimo de coordinación y coherencia entre los países. Si los distintos países llegan a un entendimiento similar acerca de lo que se entiendo por ciberdelincuencia, se mejorará la coherencia de las decisiones judiciales e impedirá la creación de paraísos seguros para delincuentes, y, además proporcionará a los institutos docentes contenido de calidad a un coste reducido.

De la información disponible de desprende lo siguiente:

- La mayoría de la oferta de formación en el empleo sólo comprende el nivel básico.
- La oferta de cursos es muy escasa, por lo que sólo llega a un número muy reducido de jueces y fiscales.
- En la mayoría de los casos, los cursos de nivel básico no están normalizados y, por ende, no pueden reproducirse ni permiten al juez o fiscal pasar de manera sistemática del nivel básico al avanzado. Los Países Bajos parece ser la única excepción.
- El material didáctico parece ser disperso y preparado para cada caso.
- Dado que en última instancia todos los jueces y fiscales necesitan adquirir al menos un nivel de conocimientos básicos sobre ciberdelincuencia y pruebas electrónicas, la oferta de formación es muy insuficiente, sobre todo teniendo en cuenta que con toda probabilidad la generación actual de jueces y fiscales en activo no han recibido formación inicial alguna sobre estos temas durante sus estudios universitarios.
- Con algunas excepciones, no se ofrece formación de nivel avanzado para jueces y fiscales.
- Dada la naturaleza internacional de la ciberdelincuencia, será necesario un nivel mínimo de coordinación y coherencia entre los países.

6 Método propuesto

6.1 Objetivo

Según se demostró en la sección precedente, en la actualidad formación inicial y en el empleo no proporciona en general a los jueces y fiscales el nivel de conocimientos necesario para tratar la ciberdelincuencia y las pruebas electrónicas.

Por consiguiente, los objetivos de la formación de jueces y fiscales en este sentido deben ser:

- Permitir a las instituciones de formación jurídica impartir formación inicial y en el empleo sobre ciberdelincuencia, con arreglo a las normas internacionales
- Dotar al mayor número posible de jueces y fiscales en activo y futuros con los conocimientos básicos en materia de ciberdelincuencia y pruebas electrónicas
- Impartir formación avanzada a un número adecuado de jueces y fiscales
- Fomentar la especialización y la formación técnica continuas de jueces y fiscales
- Contribuir a mejorar los conocimientos mediante la colaboración en red de jueces y fiscales
- Facilitar el acceso a las diferentes redes e iniciativas de formación.

Las medidas que se indican a continuación podrían contribuir a alcanzar esos objetivos.

6.2 Institucionalización de la formación inicial

- En los países donde la formación inicial consiste en formación práctica en el empleo (un tipo de contrato de prácticas o una serie de pasantías) sin un plan de estudios oficial, se recomienda que al menos una parte de dicha formación (por ejemplo, una pasantía o similar) guarde relación con la ciberdelincuencia y las pruebas electrónicas.

- En los países donde la formación inicial se imparte en instituciones de formación judicial:
  - El plan de estudios debería contener como mínimo un módulo de nivel básico sobre ciberdelincuencia y pruebas electrónicas
  - Estas cuestiones deben tratarse también en los módulos obligatorios relativos al derecho sustantivo y procesal
  - Deben ofrecerse módulos facultativos de nivel avanzado sobre ciberdelincuencia y pruebas electrónicas.

Los módulos de formación específica deben estar normalizados para que sean reproducibles y permitan a los candidatos pasar del nivel básico al avanzado. Por reproducible se entiende que otros instructores pueden impartirlo dentro del mismo país, de tal modo que los participantes en diferentes eventos de formación tengan un nivel similar de conocimientos. Esto significa además que los métodos para impartir la formación también deben estar normalizados. Para garantizar que la calidad de la formación sea constante, deberá realizarse una evaluación al final de cada curso.

6.3 Institucionalización de la formación en el empleo

- Las instituciones de formación en el empleo deberían ofrecer al menos un módulo de nivel básico sobre ciberdelincuencia y pruebas electrónicas para que los jueces y fiscales puedan adquirir los conocimientos básicos que no obtuvieron durante su formación inicial.

- También deberían ofrecer cursos de nivel avanzado.

- También en este caso, los módulos de formación específica deberían estar normalizados para que sean reproducibles y permitan a los candidatos pasar del nivel básico al avanzado. Por consiguiente, será necesario armonizar lo más posible los módulos de formación en el empleo

con los de la formación inicial. Los métodos para impartir la formación también deberían normalizarse y disponer de un control de calidad basado en evaluaciones al final del curso.

- Para formar a jueces y fiscales expertos convendría fomentar pasantías en unidades especializadas en el crimen de alta tecnología o cursos/estudios de postgrado.[12]

6.4 Cursos/módulos normalizados y reproducibles

- Deberían prepararse cursos o módulos que puedan reproducirse a gran escala de manera rentable y que permitan a los jueces y fiscales candidatos y en activo pasar del nivel básico al avanzado.

- Deberían evaluarse los cursos básicos existentes[13] para determinar si pueden integrarse en el programa de estudios de la formación inicial o en el empleo. Luego se podría recomendar un curso estándar a las instituciones que ofrecen formación inicial o en el empleo.

- Podría realizarse una evaluación similar de los cursos de nivel avanzado, para luego recomendar un curso avanzado estándar.

- Por último, podría ser necesario formar instructores para dichos cursos con el fin de lograr que sean instructores locales quienes los impartan en su idioma local y recurrir lo menos posible a instructores internacionales.[14]

6.5 Acceso a material didáctico/de autoaprendizaje

- Debería prepararse material didáctico que responda a las normas internacionales comunes y a las prácticas idóneas, y ponerlo a disposición de las instituciones docentes a buen precio para que pueda utilizarse a escala local. Es evidente que si bien es posible lograr un nivel elevado de normalización en la formación de funcionarios de las fuerzas del orden, que gira en torno a la tecnología y al análisis forense, es más difícil en cambio cuando se trata de jueces y fiscales, que han de recibir formación principalmente sobre la aplicación de la legislación nacional. No obstante, es posible crear material didáctico normalizado que sea lo suficientemente general para tener en cuenta la legislación y los sistemas nacionales.

- En algunos países, el material didáctico se publica en línea para jueces y fiscales[15], práctica que deberían adoptar otros países.

- Se deben preparar y ofrecer cursos en línea.[16]

- El acceso a los cursos de formación en línea (a nivel nacional e internacional) debe facilitarse lo más posible mediante la adopción de procedimientos de aplicación simplificados.

---

[12] Por ejemplo, el curso básico de dos semanas de duración elaborado por la policía irlandesa y el University College Dublin también sería interesante para jueces y fiscales.

[13] Por ejemplo, el curso ECCE preparado por CYBEX y que actualmente está en fase de prueba.

[14] UCD y la INTERPOL han elaborado un curso para "formar instructores" que podría publicarse. El curso trata de las competencias didácticas, el desarrollo del curso, etc. No se trata de un curso destinado exclusivamente a las fuerzas del orden sino que podría impartirse a cualquiera.

[15] Ejemplos son los Países Bajos y la biblioteca de pruebas electrónicas de CYBEX. En el marco del proyecto 2CENTRE, UCD preparará cursos en línea para suministrar material didáctico de AGIS/ISEC.

[16] Por ejemplo, UCD ofrece actualmente dos programas de Master of Sciences, parte de los cuales se imparten totalmente en línea. El CEJ de Portugal tiene previsto organizar un curso en línea sobre los Tribunales y las TIC, que incluye módulos sobre ciberdelincuencia y pruebas electrónicas. El curso se impartirá en portugués y se está considerando la posibilidad de exportarlo a otros países de habla portuguesa (por ejemplo, Brasil, Cabo Verde, Angola, Mozambique, Guinea-Bissau, Santo Tomé o Timor).

6.6 Centros piloto para la formación básica y avanzada

- Deberían crearse varios centros piloto para la formación básica y avanzada de jueces y fiscales en materia de ciberdelincuencia y pruebas electrónicas, en los que se podría:
  - probar y mejorar cursos y material didáctico normalizado
  - divulgar prácticas óptimas
  - realizar investigación sobre formación
  - mantener un registro de instructores
  - ofrecer formación a instructores
  - impartir formación a otros países con sistemas e idiomas similares.

- Los centros piloto deberían coordinar sus actividades entre sí, con la asistencia del Consejo de Europa.

- Los jueces y fiscales que deseen convertirse en expertos deben considerar la posibilidad de participar en la formación que ofrezcan los centros de excelencia a las fuerzas del orden y al sector privado.[17]

6.7 Mejorar los conocimientos mediante la colaboración en red

Si bien la formación inicial y en el empleo proporcionará a jueces y fiscales los fundamentos también será esencial la cooperación y la colaboración en red entre jueces y fiscales, así como con otros interesados.

Así pues:

- Jueces y fiscales deberían utilizar las redes de jueces [18] y fiscales existentes (como la red GPEN).[19]
- El Consejo de Europa debería considerar la posibilidad de crear una red internacional de jueces especializados en ciberdelincuencia y delitos electrónicos (similar a la red GPEN para fiscales).
- El Consejo de Europa y la Red Europea de Formación Judicial deberían fomentar la colaboración en red de las instituciones europeas que ofrecen formación sobre ciberdelincuencia y pruebas electrónicas.

[17] La Iniciativa 2Centre (Red de Centros de Excelencia para la investigación en formación y la educación) fue lanzada en marzo de 2009 (durante la Conferencia Octopus del Consejo de Europa). En esta iniciativa "se examinan los métodos actuales que emplean las fuerzas del orden y la industria en la informática forense y la investigación de ciberdelincuencia. Se analizan las actividades realizadas por miembros del personal de las fuerzas del orden y de la industria pertinente para obtener conocimientos y competencias en una esfera en la que actualmente existen una gran diversidad de niveles de formación profesional, formación interna, formación cruzada y aprendizaje en el empleo". El primer centro de excelencia es la University College Dublin; la Universidad de Troyes se convirtió en el segundo en 2010.

[18] Al parecer aún no existe una red internacional para jueces que trate de la ciberdelincuencia y las pruebas electrónicas. Como ejemplo de iniciativa nacional puede citarse el desarrollado en los Países Bajos donde se ha creado un recurso Intranet del tipo wiki.

[19] La Red Global de Ciberdelincuencia de la Fiscalía (GPEN), es una iniciativa creada en 2008 bajo los auspicios de la Asociación Internacional de Fiscales (IAP). La finalidad de la red es facilitar el intercambio de información y la cooperación en casos que guarden relación con los delitos electrónicos o la ciberdelincuencia, teniendo en cuenta el Convenio sobre la Ciberdelincuencia, elaborar y suministrar programas de formación, y proporcionar recursos en línea a los fiscales. GPEN es una red de fiscales expertos en ciberdelincuencia. Se ha invitado a cada organización miembro de la IAP que nombren al menos un fiscal que quedará registrado como punto de contacto nacional de la GPEN. La red está gestionada por la Junta de Desarrollo de GPEN constituida a partir de los miembros de la IAP.

- Para facilitar a los jueces y fiscales el acceso a éstas y otras muchas redes relacionadas con la ciberdelincuencia, el Consejo de Europa – en su sitio www.coe.int/cybercrime - debería elaborar un registro de iniciativas y redes, y crear un portal con enlaces, información sucinta e información de contacto acerca de las distintas redes. Este portal facilitará, además, la coordinación entre las redes y el acceso a las iniciativas y al material didáctico existente.

6.8 Cooperación entre los sectores público y privado

La cooperación estructurada y reglamentada entre las fuerzas del orden y el sector privado (la industria de las TIC, incluidos los proveedores de servicios Internet) es fundamental para la investigación de la ciberdelincuencia y la obtención de pruebas electrónicas[20]. El sector privado puede aportar la experiencia y contribuir a las iniciativas de formación de las fuerzas del orden.

El apoyo del sector privado a la formación de jueces y fiscales también sería útil, por cuanto el sector privado dispone de gran experiencia sobre este particular. Por otra parte, debe mantenerse la independencia e imparcialidad de los jueces y fiscales.

Así pues:

- Las instituciones de formación judicial pueden aprovechar la experiencia del sector privado al concebir programas de formación, preparar material didáctico e impartir cursos.

- La colaboración del sector privado con las instituciones docentes no debe aprovecharse para obtener posibles decisiones favorables en los tribunales o hacer negocio, sino para garantizar que los jueces y fiscales reciben la información adecuada que les permita tomar decisiones con conocimiento de causa.

- El sector privado podría ayudar de manera transparente a organizaciones internacionales o nacionales, universidades, iniciativas de formación o a terceros que luego colaborarán con instituciones docentes independientes.

- Si bien los jueces y fiscales deben disponer de conocimientos generales sobre Internet y ciberdelincuencia, también es importante proporcionarles información relativa a plataformas específicas. La industria podría ofrecer material para módulos específicos (en lugar de cursos completos) sobre el funcionamiento de las principales plataformas.

[20] Véase, por ejemplo, las directrices para las fuerzas del orden público – Cooperación de los PSI, adoptadas en la Conferencia Octopus del Consejo de Europa el mes de abril de 2008.

7 Ayudar a la poner en práctica esta idea

La puesta en práctica de esta idea es responsabilidad, sobre todo, de las instituciones de formación judicial, pero debería contarse con el apoyo de instituciones y asociados de los sectores público y privado, en particular las organizaciones internacionales. Habida cuenta de la importancia que revisten las tecnologías de la información y la comunicación para la sociedad, la financiación de tales medidas de formación será una buena inversión, por lo que debería hacerse todo lo posible para proporcionar a las instituciones de formación los recursos necesarios.

El Consejo de Europa y la Red Europea de Formación Judicial (REFJ), así como otros órganos, deben promover la aplicación de esta idea en Europa y otras regiones.

La REFJ y el Consejo de Europa podrían organizar en el futuro inmediato una conferencia mixta sobre esta idea.

El Consejo de Europa y la REFJ deben evaluar regularmente los progresos.

La puesta en práctica de esta idea también debe contar con la colaboración de donantes. Las organizaciones y los donantes interesados podrían asociarse para elaborar proyectos destinados a prestar asistencia a las instituciones de formación y otras partes interesadas dispuestas a adoptar las medidas propuestas dimanantes de esta idea y asumir las correspondientes responsabilidades.

A los efectos de reducir el riesgo de que se produzcan conflictos de intereses o poner en peligro la imparcialidad de jueces y fiscales, los donantes podrían proporcionar los recursos por mediación de terceros independientes, en lugar de ofrecerlos directamente, por ejemplo a organizaciones internacionales que luego cooperarán con las instituciones de formación.

8 Anexo

8.1 Red de Lisboa: enlaces a instituciones de formación judicial

Cuarenta y cuatro de los cuarenta y siete Estados miembros del Consejo de Europa están representados en la Red de Lisboa. Los miembros de la Red de Lisboa son las instituciones nacionales encargadas de la formación inicial y continua de jueces y fiscales. También puede tratarse, según el caso, de Escuelas de Magistrados, Centros de formación jurídica o servicios de formación de magistrados de los Ministerios de Justicia.

Para mayor información sobre cada país miembro de la Red (con inclusión, en ciertos casos, de los correspondientes programas de formación), véase:

- Albania
- Alemania
- Andorra
- Armenia
- Austria
- Azerbaiyán
- Bélgica
- Bosnia y Herzegovina
- Bulgaria
- Chipre
- Croacia
- Dinamarca
- Eslovaquia
- Eslovenia
- España
- Estonia
- Federación de Rusia
- Finlandia
- Francia
- Georgia
- Grecia
- Hungría
- Islandia
- Irlanda
- Italia
- Letonia
- Lituania
- Luxemburgo
- "la ex República Yugoslava de Macedonia"
- Malta
- Moldova
- Montenegro
- Noruega
- Polonia
- Países Bajos
- Portugal
- República Checa
- Rumania
- Serbia
- Reino Unido
  - Inglaterra y el País de Gales
  - Escocia
- Suecia
- Suiza
- Turquía
- Ucrania

Observador

- MINUK

8.2 Ejemplos de cursos de formación básica: estructura y temas de estudio

8.2.1 Ejemplo de Países Bajos

<u>Formación básica</u> – 1 día
Programa:

1 Orientación general:
- Qué es la ciberdelincuencia
- Manifestación de la ciberdelincuencia
- Marco jurídico para la aplicación de la ley y el procesamiento

2 Aplicación de la ley:
- Aplicación de la ley digital como práctica cotidiana
- Métodos de aplicación de la ley

3 Aplicación de la ley (parte 2):
- Internet y aplicación de la ley en el marco de la Ley sobre privilegios especiales de aplicación de la ley

Conclusiones + evaluación

8.2.2 Ejemplo de Alemania (Escuela Judicial Alemana)

<u>Formación básica:</u> ***"Formas de manifestación y estrategia para luchar contra la ciberdelincuencia*** **" – 4 días**
Programa:

<u>1º día:</u>
- Código Penal Alemán
- Utilización del Código Penal Alemán en el contexto de la delincuencia informática y de Internet
- Problemas cotidianos en la fiscalía y los tribunales

El orador es un juez del Tribunal de Munich experto en delitos financieros y económicos, que hace algunos años era fiscal encargado de casos de ciberdelincuencia, espionaje de datos, alteración de datos, etc.

- Problemas cotidianos en la fiscalía y los tribunales de los Países Bajos
- Evolución y lucha contra la ciberdelincuencia en Europa
- Problemas con los proveedores en los Países Bajos y otros países europeos
- Convenio sobre la ciberdelincuencia del Consejo de Europa
- Importancia y significado del Convenio sobre la ciberdelincuencia para Europa y el resto del mundo (China, Estados Unidos, Rusia)

El orador es el Dr. Henrik Kaspersen, de Países Bajos

<u>2º día</u>:
- Sabotaje de sistemas informáticos
- Pirateo por Internet
- Trampas en pedidos por Internet
- Espionaje de datos
- Fraude informático con tarjetas de crédito
- Ataques a datos bancarios
- *Peska* (*phishing*) y nuevos tipos de delitos en Internet
- Redes robot
- Fraude por eBay y otras plataformas de compraventa

El orador es un policía del Cuartel de la Policia Alemana (BKA) de Wiesbaden

- Búsqueda preventiva en Internet del crimen organizado, terrorismo, delitos graves, lavado de activos, etc.

- Búsqueda en Internet de anuncios de personas con el síndrome Amor (escuelas, etc.)
- Búsqueda en Internet de pornografía infantil
- Cooperación internacional en la investigación por la red
- Búsqueda en línea (problemas con la constitución)

El orador es el director del departamento especial del cuartel de la policía de Baviera (LKA Munich)

3 día:

- Copia de seguridad y análisis de datos en Alemania y otros países
- Búsqueda de datos en Internet y rastreo de datos en la red
- Posibilidades de la informática forense y límites del análisis de datos
- Sistemas para obtener datos anónimos en la red
- Cripotogramas utilizados por los delincuentes

El orador es un experto del cuartel de la policía de Munich

- Nuevos problemas jurídicos de la copia y análisis de datos de Internet
- Facultad de todas las medidas jurídicas de búsqueda
- Facultad de obtener pruebas para la investigación y para tribunales
- Nuevos adelantos en la aplicación de la ley

El orador es un juez del Tribunal Penal Supremo de Baviera en Bamberg

4º día:

- Red empresarial de Rusia
- Intercage
- Protección contra el sabotaje de ordenadores o datos
- "Pirateo" positivo
- Influencia y falsificación de máquinas electorales
- Influencia política en la nueva legislación
- Población en una casa de cristal

El orador es un miembro del famoso Club Informático Caos (CCC) de Hamburgo, cuyos miembros se dedican a tratar de entrar en los ordenadores del gobierno, la Casa Blanca y la CIA. El club ha demostrado cómo manipular el suministro de agua de una ciudad, etc.

8.2.3 Ejemplos del Consejo de Europa

1. Taller de formación sobre ciberdelincuencia, Belo Horizonte, Brasil, 26 de agosto de 2008 (organizado por el Ministério Publico Estadual Minas Gerais en cooperación con el Consejo de Europa)

Formación básica – 1 día

Programa:

1 Sesión de apertura
- Discursos de apertura
- Reforma de la legislación actual

2 El fenómeno de la Ciberdelincuencia
- Descripción general de las actuales amenazas
- Amenazas concretas y casos investigados en Brasil

3 Derecho sustantivo: ¿qué se considera delito?
- Normas internacionales
  - Tipología, conceptos jurídicos
  - Convenio sobre la ciberdelincuencia
- Disposiciones en la legislación de Brasil
  - Disposiciones vigentes
  - Reforma jurídica en curso

4 Investigaciones y cooperación internacional
- Función de los fiscales en la investigación de ciberdelitos
- Derecho procesal nacional
- Medidas procesales y cooperación internacional prevista en el Convenio sobre la ciberdelincuencia

5 Asociación entre los sectores público y privado
- Ejemplos de asociación entre los sectores público y privado en Brasil
- Aplicación de la ley – Cooperación de los proveedores de servicios Internet en la investigación de ciberdelitos: directrices
- Debate: aplicación de la ley – cooperación de los PSI: experiencia en Brasil

2. Ciberdelincuencia: formación de jueces, El Cairo (Egipto), 9 y 10 de junio de 2008 (organizado por Microsoft con la participación del Consejo de Europa)
Este curso se ha impartido en dos ocasiones por distintos grupos de jueces de tribunales mercantiles (que también se encargan de la ciberdelincuencia)

Formación básica – 1 día

Programa:

1 Sesión de apertura

2 El fenómeno de la ciberdelincuencia
- Descripción general de las amenazas actuales
- Amenazas específicas
  - Utilización fraudulenta de identidades e información en línea: ejemplos
  - Fraudes con tarjetas de crédito y otros tipos

3 Derecho sustantivo: ¿qué se considera delito?
- Normas internacionales (experto del Consejo de Europa)
  - Tipología, conceptos jurídicos
  - Convenio sobre la ciberdelincuencia
  - Acusación de robo de identidad
- Disposiciones en la legislación nacional
  - Disposiciones actuales
  - Reforma jurídica en curso

2ª parte – Pruebas en los procesos

4 Investigaciones y acciones penales
- Medidas procesales previstas en el Convenio sobre la ciberdelincuencia
- Función de la policía, los fiscales, los jueces, los servicios especiales
- Derecho procesal nacional

5 Cooperación internacional

- Convenio sobre la ciberdelincuencia
- Disposiciones previstas en el derecho nacional y los acuerdos bilaterales
- Puntos de contacto 24/7
- Función de los jueces

6 Obtención, conservación y utilización de pruebas electrónicas
- Pruebas en el ordenador de la persona acusada: presencia de archivos digitales utilizados para cometer el ciberdelito
- Pruebas que identifican la ubicación de la red: direcciones IP
- Pruebas obtenidas de los proveedores de servicios Internet

7 Procedimientos judiciales y jurisprudencia: ejemplos

8.3 Ejemplos de cursos de formación avanzados: estructura y temas tratados

8.3.1 Ejemplo de los Países Bajos

Formación avanzada – 4 días
Programa:

1º y 2º días

La infraestructura de Internet

- Cómo funciona Internet
- Cómo se comunican los ordenadores
- Qué son los números IP y los nombres de los ordenadores

Información en Internet

- Cómo recabar información por Internet
- Búsqueda de bases de datos (ocultas) de Internet

Características de las redes sociales

- comunicación
- anonimato
- determinación de la ubicación y la identidad de los ordenadores, las empresas y las personas en Internet

Huellas digitales

- ¿Qué son las "huellas"?
- ¿Qué huellas se dejan en un ordenador?
- ¿Qué huellas se dejan en Internet?
- ¿Qué huellas pueden encontrarse en una comunicación digital?

Seguridad

- Los riesgos de Internet
- La importancia de una gran seguridad digital
- Almacenamiento seguro de la información
- Seguridad en el correo electrónico

Durante estos dos días cada participante tiene acceso a un ordenador conectado a Internet y dispone de experiencia en los temas tratados. Se dará a los participantes el nombre de una persona y se les pedirá que averigüen la toda la información posible sobre ella, utilizando todas las fuentes de acceso libre disponibles en Internet. También se les pedirá rastrear los orígenes de un mensaje de correo electrónico (a partir de los encabezados) o seguir la pista de una comunicación digital.

3º y 4º días

Marco jurídico

- Cuáles son las competencias de la policía y los fiscales que investigan la ciberdelincuencia
- Estudio de caso presentado un el equipo de delitos de alta tecnología

La Organización de investigación y procesamiento de ciberdelincuencia en los Países Bajos;

Intercepción (este tema no se tratará en el nuevo curso, dado que pasará a formar parte del programa básico);

Alegatos de defensa digital

- Qué alegatos de defensa se conocen
- Jurisprudencia sobre esos alegatos

- Qué alegatos de defensa cabe esperar en el futuro y cómo responder a los mismos
- Estudios de caso

Se facilitará a cada participante material didáctico, un libro de lectura que contiene todos los temas discutidos durante la formación y que puede utilizarse como libro de referencia, todas las presentaciones impresas utilizadas por los instructores y el libro Handboek Digitale Criminaliteit del autor Arjan Dasselaar.

8.3.2 Propuesta de curso avanzado formulada por los Países Bajos

Preparación de un nuevo curso sobre ciberdelincuencia

El 'Intensiveringsprogramma Cybercrime', la Fiscalía Nacional sobre ciberdelincuencia y el SSR (Centro de Formación Judicial Holandés) han estado preparando un nuevo curso sobre ciberdelincuencia que trata de temas diversos, desde la 'intercepción' hasta cursos avanzados sobre temas específicos de ciberdelincuencia (redes robot).

Aún no se terminado de definir el programa, pero el primer día se tratarán los fundamentos de la intercepción (intervención de cables y de Internet), y el segundo consistirá en un curso básico sobre ciberdelincuencia. Estos dos cursos serán obligatorios para *todos* los fiscales en los Países Bajos y formará parte de su educación continua. La segunda parte del curso estará destinada exclusivamente a expertos en ciberdelincuencia (se aplicarán criterios de admisión estrictos) y consistirá en un curso avanzado (de 2 a 4 días) y una clase principal de dos días de duración (al año). Estos cursos se imparten con la colaboración de asociados externos, tales como Fox-IT, Digital Intelligence Training y Hoffman Bedrijfsrecherche.

La preparación de este curso no se debe a que el contenido de la formación impartida hasta ahora sea insatisfactorio, sino a la voluntad de mejorar la estructura de las distintas partes del curso y evitar que haya duplicaciones. Otra razón importante por la que se preparó/reestructuró la formación fue el nombramiento, en el marco del "intensiveringsprogramma" de fiscales especializados en ciberdelincuencia en once de las oficinas más grandes de la Fiscalía Holandesa. Otro aspecto esencial del nuevo curso es que existe una progresión, es decir, cada participante debe terminar los dos cursos básicos antes de poder ser admitido en los cursos de nivel intermedio y avanzado.

Una de las nuevas características previstas en la nueva formación será la información gráfica sobre el funcionamiento y los riesgos que entraña Internet. Esta información gráfica se encuentra en las últimas fases de desarrollo y puede utilizarse en presentaciones de prueba. A continuación se muestran dos ejemplos de cuál es el aspecto de la información gráfica.

Seguimiento

Para garantizar que los fiscales que se ocupan de la ciberdelincuencia en su práctica cotidiana pueden mantenerse al corriente de los últimos adelantos que se producen en el mundo de la ciberdelincuencia que evoluciona rápidamente, se están llevando a cabo dos programas adicionales.

El primero consiste en la creación de un centro de conocimientos y experiencia en la Fiscalía Nacional de Rotterdam. En este centro se atenderán las preguntas técnicas y de índole jurídica, se mantendrán al corriente de la jurisprudencia más reciente y distribuirá ésta y otra información a

todos los profesionales de la ciberdelincuencia, tanto de las fuerzas de la policía como de la fiscalía (el centro pertenece a ambas organizaciones).

El segundo, anexo a este proyecto consiste en la creación de una 'sala digital de cooperación', comparable a la aplicación Sharepoint. En esta sala virtual los profesionales en estos temas pueden debatir acerca de cuestiones relativas a su trabajo y encontrar información de todo tipo importante para su trabajo. En octubre de este año se analizará qué contenido y posibilidades (técnicas) debe tener la sala digital. Este es un ejemplo de qué aspecto podría tener la página de inicio de la sala digital:

Creación de un sentido de urgencia: formación a nivel directivo

Dada la capacidad relativamente pequeña de las fuerzas de la policía holandesa, es necesario decidir qué delitos investigar y cuáles no (obsérvese que el sistema jurídico holandés permite a la fiscalía no investigar y enjuiciar ciertos delitos, lo que se denomina opportuniteitsbeginsel). Por lo general las decisiones se toman a nivel directivo.

La policía y la Fiscalía reconocen que a este nivel existe una falta de conocimientos sobre las repercusiones de la ciberdelincuencia y la importancia de combatirla, y que existe el riesgo de que no se investiguen casos importantes porque se estima que otros delitos (convencionales) revisten más importancia. Por consiguiente, se está elaborando un curso de formación destinado al personal directivo de la policía y la fiscalía. Según las previsiones, a finales de año se impartirá la formación a título de prueba. La finalidad de esta formación es lograr que los participantes sean conscientes de lo urgente que es luchar contra la ciberdelincuencia y confrontarlos con la realidad de este fenómeno en la sociedad de hoy en día. Los temas no se tratarán a nivel de contenido (como en el caso de la formación avanzado), sino más bien en el plano de dirección y estrategia.