aec²

THE ADMISSIBILITY OF
ELECTRONIC EVIDENCE IN COURT
CYBEX INITIATIVE

LA ADMISIBILIDAD DE LAS PRUEBAS ELECTRÓNICAS ANTE LOS TRIBUNALES:
LUCHANDO CONTRA LOS DELITOS TECNOLÓGICOS

THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT:
FIGHTING AGAINST HIGH-TECH CRIME

L'ADMISSIBILITÉ DE LA PREUVE ÉLECTRONIQUE DEVANT LES TRIBUNAUX :
LUTTE CONTRE LES DÉLITS TECHNOLOGIQUES

AGIS 2005
With financial support from the AGIS Programme
European Commission -Directorate- General Justice,
Freedom and Security

cybex
Intelligence on e-evidence

INVESTIGADOR PRINCIPAL / MAIN INVESTIGATOR
INVESTIGATEUR PRINCIPAL

FREDESVINDA INSA
CYBEX

COORDINACIÓN / COORDINATION

CARMEN LÁZARO
CYBEX

EQUIPO INVESTIGADOR / RESEARCH TEAM
ÉQUIPE D'INVESTIGATION

BURKHARD SCHAFER
UNIVERSITY OF EDINBURGH
CYBEX
DAN MINZALA
NATIONAL INSTITUT OF CRIMINOLOGY OF ROMANIA
DIEGO TORRENTE
UNIVERSIDAD DE BARCELONA
FERNANDO FERNÁNDEZ
POLICÍA NACIONAL DE ESPAÑA
FRANCISCO MÁLAGA
UNIVERSIDAD POMPEU FABRA
FREDESVINDA MÉRIDA
UNIVERSIDAD DE BARCELONA
JOHN KINGSTON
UNIVERSITY OF EDINBURGH
PATRICK BURKE
QINETIQ
SHARA MONTELEONE
ASSOCIAZIONE NAUTILUS

COLABORACIÓN / COLLABORATION

FLORENCIA RODRÍGUEZ -CYBEX-
NURIA GARCÍA -CYBEX-

PRIMERA EDICIÓN, 2006
FIRST EDITION, 2006
PREMIÈRE ÉDITION, 2006

LA ADMISIBILIDAD DE LAS PRUEBAS ELECTRÓNICAS ANTE LOS TRIBUNALES:
LUCHANDO CONTRA LOS DELITOS TECNOLÓGICOS

THE ADMISSI
ELECTRONIC
CYBEX INITIATIV

INTRODUCCIÓN

Las nuevas tecnologías y la evolución de los sistemas de comunicación han transformado sustancialmente los procesos de intercambio de información y producción, en todas las esferas de la vida: empresarial, civil y militar, aumentando exponencialmente la creación de documentos electrónicos en las organizaciones. Anualmente se envían en todo el mundo más de tres trillones de correos electrónicos y más del 90% de los documentos creados en las organizaciones son electrónicos, de los que menos del 30% se imprimen.

El uso masivo de los medios digitales y del entorno virtual no está exento de conflictos, ni de usos fraudulentos o criminales. Las tipologías tradicionales de fraudes y delitos se han modificado al utilizar nuevos canales de comunicación e incorporar nuevas categorías delictivas. Delincuentes y bandas organizadas han encontrado en los nuevos medios tecnológicos un firme aliado para la comisión de crímenes, tales como la pornografía infantil a través de Internet, el *phishing*, el *pharming,* el abuso de medios corporativos y competencia desleal, entre muchos otros.

Ante estas nuevas vías de comisión y tipos de delitos, aparece una nueva herramienta que permite probar dichos fraudes: la *prueba electrónica*. Instrumento que, poco a poco, está pasando a formar parte de nuestra vida diaria y está adquiriendo una mayor importancia en los procesos judiciales. Se puede afirmar que las pruebas tradicionales están migrando desde el soporte papel hacia un entorno virtual y sus procesos de gestión y criterios de admisibilidad cambian con respecto a la prueba tradicional.

Asumimos que la *prueba electrónica* es el medio adecuado para probar la comisión de los delitos cometidos a través de las nuevas tecnologías, y la definimos *como cualquier información obtenida a partir de un dispositivo electrónico o medio digital que sirve para adquirir convencimiento de la certeza de un hecho.*

Debido a la importancia de esta nueva herramienta procesal, consideramos que era fundamental ahondar en el conocimiento de la admisibilidad de las *pruebas electrónicas* ante los tribunales, como medio para luchar contra los delitos tecnológicos. Por ello, el objetivo del proyecto era dar respuesta a las siguientes preguntas fundamentales: ¿qué es la *prueba electrónica*?, ¿está regulada la *prueba electrónica* en Europa?, ¿qué problemas tienen los agentes sociales europeos implicados en la obtención, análisis y presentación de las *pruebas electrónicas* y cómo están actuando en realidad? Las respuestas a estas preguntas permitirán llegar a conocer la realidad tanto legislativa como práctica en esta materia. Estos objetivos, justificaron que, la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea, dentro del Programa Marco AGIS, aprobara nuestro proyecto debido al valor añadido que representa, que por primera vez se estudie a nivel europeo un instrumento jurídico que, cada día más, afecta a los ciudadanos europeos. Además, con esta investigación se desarrolla y refuerza el *networking* entre estados de la UE y países candidatos. Permite el intercambio de información y experiencias a nivel europeo a la vez que la cooperación entre autoridades judiciales, abogados, policías y expertos privados. Es una forma de contribuir al desarrollo y consolidación del Espacio Judicial Europeo, luchando conjuntamente contra los delitos tecnológicos.

Un proyecto ambicioso y novedoso que se ha llevado a cabo en dieciséis países, los quince países de la Unión Europea[1] y Rumania, como Estado candidato a la Unión Europea. Un equipo de investigadores multidisciplinares europeos (policías, juristas, sociólogos, técnicos, empresarios, académicos, abogados y expertos en informática forense), asumimos como reto profesional y nos comprometimos a desarrollarlo en un año.

Para realizar el análisis legal de la *prueba electrónica* y su admisibilidad ante los tribunales y conocer el grado de desarrollo y homogeneidad legislativa alcanzado en Europa, hemos procedido a hacer una revisión de las legislaciones en vigor. El campo de observación lo forman las normas, que de alguna manera tratan y afectan a alguno de estos cuatro elementos: "prueba", "*prueba electrónica*", "admisibilidad de la prueba" y "admisibilidad de la *prueba electrónica*". Las normas analizadas siguiendo este criterio han sido setenta y ocho.

Para conocer los problemas con los que se encuentran los agentes sociales que intervienen en un análisis forense de medios electrónicos y cómo están actuando, se han realizado ciento veinticinco entrevistas en profundidad a los siguientes perfiles: abogados, jueces civiles, penales, mercantiles y laborales, fiscales, notarios, representantes del Consejo General del Poder Judicial, policías, expertos en informática forense y empresarios, recogiendo sistemáticamente la información que nos han transmitido. Finalmente, con toda la información legal y práctica obtenida hemos realizado una guía de mejora.

La investigación es un estudio comparado de derecho procesal, concretamente en las disposiciones relativas a la admisibilidad de las *pruebas electrónicas* ante los tribunales. El objetivo es conocer las lagunas existentes e identificar las mejores prácticas para conseguir una mayor protección de los intereses de las víctimas en los procedimientos,

[1] Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Holanda, Irlanda, Italia, Luxemburgo, Portugal, Reino Unido, Rumania y Suecia.

desarrollando la *prueba electrónica* como una herramienta útil para luchar contra los delitos tecnológicos.

Antes de proceder a la presentación de los resultados obtenidos, tenemos que comentar las limitaciones que hemos identificado en esta investigación. Este estudio se circunscribe dentro de los parámetros propios del análisis de contenido de las leyes europeas que contemplan la *prueba electrónica*, pero no se revisan los efectos sociales de las mismas. Tampoco hemos analizado el impacto social que haya podido generar las estructuras de relaciones jurídicas que se crean a través de las leyes y sus elementos más significativos. Una de las dificultades que hemos tenido que superar hace referencia a la pluralidad lingüística europea. Consensuamos trabajar en inglés ya que muchas de las leyes ya estaban traducidas a este idioma, sin embargo otras muchas sólo existen en el idioma propio del país en el que fueron publicadas. Finalmente, debemos destacar, la dificultad principal intrínseca de un estudio de derecho comparado debido a que no todas las figuras y/o elementos jurídicos tienen la misma/idéntica equivalencia en cada ordenamiento jurídico. Superadas algunas de estas limitaciones y teniendo en cuenta las dificultades encontradas, hemos conseguido unos resultados que nos han permitido desarrollar una propuesta de "guía de mejora", que, entendemos, será una referencia a considerar por los profesionales europeos.

DATOS Y MÉTODO

El Derecho Procesal Comparado junto con la Sociología del Derecho son los marcos teóricos elegidos en la presente investigación. Para conocer la realidad jurídica y práctica de la *prueba electrónica* en Europa se ha analizado el contenido de las leyes y las relaciones cognitivas que se crean entre los elementos significativos que componen esas normas. Teniendo en cuenta que la organización cognitiva del conjunto de elementos es diferente en cada normativa y país, hemos elegido distintos materiales y métodos de análisis.

Para el análisis de la legislación hemos creado un cuestionario a tal efecto, sistematizando la recogida de la información proveniente de datos secundarios. Los *datos secundarios* están constituidos por las legislaciones de dieciséis países europeos que regulan la prueba, la *prueba electrónica, la admisibilidad de la prueba o la admisibilidad de la prueba electrónica*.

Para el estudio de la realidad hemos recogido los siguientes *datos primarios*:

a) Datos procedentes de una encuesta presentada a una muestra de profesionales relacionados al análisis forense de medios electrónicos y su admisibilidad, como una aproximación inicial a la noción de *prueba electrónica.* Se trata de una muestra no representativa estadísticamente. Es una aproximación prospectiva y las personas se eligen en entornos próximos al uso de este tipo de prueba. Todas las personas participantes han sido seleccionadas por cumplir los requisitos en los tres perfiles consensuados por los investigadores. No obstante, el campo de observación está formado por los actores sociales implicados: abogados, fiscales, jueces (civil, penal, mercantil, laboral) representantes del poder judicial, notarios, policía, expertos en informática forense y empresarios. El objetivo es el acercamiento prospectivo a los descriptores básicos de la *prueba electrónica*

b) Datos procedentes de *entrevistas en profundidad,* como mínimo a un representante de cada grupo profesional en cada uno de los dieciséis países estudiados. Se trata de una muestra cualitativa, que es seleccionada directamente por cada investigador. El objetivo es reunir, en cada país, un abanico que sea diverso y heterogéneo de participantes, que puedan expresar opiniones diferentes respecto a cómo están actuando en su práctica, ventajas, inconvenientes y perspectivas de futuro cuando tratan con *pruebas electrónicas*. Para esta parte del trabajo de campo, se han utilizado tres protocolos diferentes, uno para juristas, otro para expertos en informática forense y otro para empresarios.

   En total, la muestra del campo de observación está constituida por ciento veinticinco cuestionarios y setenta y ocho leyes.

Las estructuras están formadas por las relaciones que forman los elementos jurídicos contenidos en las leyes que regulan la *prueba electrónica* en Europa. Se crean "a través" y "en" las leyes escritas, que era uno de los objetivos en la recogida de datos secundarios. Buscamos el universo semántico de la conceptualización jurídica de la *prueba electrónica* mediante asociación de palabras o términos utilizados para definir el concepto y uso de estas pruebas.

En el proceso de investigación hemos utilizados el análisis de contenido tradicional y el análisis estructural o de redes semánticas o cognitivas. Este último, es una metodología de última generación que centra su atención en la interacción entre los elementos observados[2], sea cual sea su nivel de agregación (significantes, individuos, grupos, u organizaciones). A través de las estructuras relacionales se explican los procesos jurídicos y los comportamientos de los profesionales en Europa. Se conectan, se ponen en relación los elementos relevantes[3]. Es una aproximación metodológica que se aleja de los procesos intuitivos. Explicar los procesos y comportamientos sociales con relación a la red de relaciones que conectan a elementos jurídicos y actores, es una nueva aproximación teórica del conocimiento científico. Las redes cognitivas se construyen a partir de los elementos jurídicos que son compartidos en las leyes que regulan la *prueba electrónica*. Permite adquirir una visión de conjunto sobre la relevancia que legisladores y profesionales europeos confieren a cada elemento. En el presente estudio se desarrolla una forma innovadora y sugerente de presentación y elaboración de la información, que puede orientar hacia aspectos y dimensiones de interés en el marco general de análisis de la regulación de la *prueba electrónica*. Permite además identificar de forma rápida y visual, entre gran cantidad de información, una o varias representaciones de la noción que se investiga, y comparar entre las mismas, o entre varias nociones en los distintos documentos en los que se aplica el análisis.

A) SOBRE LA PRUEBA ELECTRÓNICA

El uso de *pruebas electrónicas* se ha convertido en un elemento necesario para tratar de esclarecer delitos cometidos con o a través de dispositivos electrónicos. Por consiguiente, hemos profundizado en la regulación de la *prueba electrónica* a través de las referencias encontradas en los textos legales de Europa y Rumania respecto a la prueba en general o prueba tradicional, a los medios de prueba, al documento electrónico y a la firma electrónica.

Las referencias legales resultan de aplicación a la *prueba electrónica* gracias al principio interpretativo de la aplicación analógica de las normas, presente en los sistemas jurídicos, que permite utilizar las disposiciones legales para regular una situación específica o una laguna legislativa. El principio de aplicación analógica de las normas adquiere una relevancia muy especial en el análisis de la legislación en Europa en materia de *prueba electrónica* debido a que no existen normas específicas para este tipo de prueba. Los hallazgos encontrados en las normas han sido corroborados por las respuestas obtenidas en la práctica: la mayoría de los jueces entrevistados se basan en este concepto interpretativo para tratar de dar una solución jurídica a los casos en los que se les presentan este tipo de pruebas.

Definición de *prueba electrónica*

La revisión legislativa realizada muestra que no se han encontrado referencias directas y explícitas a la *prueba electrónica* ni una definición *per se,* específica y exclusiva. Sin embargo, en todos los países hay normas que contienen preceptos que, de alguna manera, hacen referencia a la *prueba electrónica*.

En el caso de Alemania, el *Código de Procedimiento Penal* contiene artículos aplicables a la *prueba electrónica*, concretamente, disposiciones relativas a la protección de datos durante una investigación. Los artículos detallan las condiciones de destrucción de datos sin interés específico para el caso. Este texto incluye también preceptos sobre las medidas a seguir a la hora de guardar datos personales obtenidos en investigaciones en las bases policiales.

El *Código de Procedimiento Penal* vigente en Austria incluye una serie de normas, de condiciones y requisitos que deben cumplirse para acordar medidas de *observación de las telecomunicaciones*.

[2] Rodríguez, 2005, Mérida, 2004.

[3] Wasserman, 1994; Borgatti, Everett y Freeman 1996; Freeman, Borgatti y White,1991; Burt 1997, 1992, 1982.

En Bélgica la *Ley relativa a los Delitos Informáticos* enuncia que las normas referentes a la recogida de pruebas bajo esta Ley son aplicables a todo tipo de pruebas y por lo tanto, también a las electrónicas.

En el caso de la *Legislación Procesal Civil* holandesa, se establece que *la prueba puede ser introducida por cualquier medio, salvo que esté explícitamente prohibido por Ley.*

En España la *Ley de Enjuiciamiento Penal* incluye entre los medios de prueba *los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.* Además, en la enumeración de los diferentes soportes que pueden considerarse un "documento" bajo el *Código Penal* se incluye *cualquier soporte que contenga datos*. Por último en España, la *Ley de Procedimiento Laboral* permite el uso de todo tipo de pruebas, inclusive aquellos *medios mecánicos de reproducción de palabras, imágenes y sonidos*.

En el *Código de Procedimiento Judicial finlandés*, cuando se habla de la carga de la prueba, se refiere a ésta como *los hechos que apoyan la acción,* entendiendo por "hecho" tanto el digital como el tradicional. Además, la regulación de Finlandia contiene una definición de mensaje electrónico, al que se refiriere como *aquella información que ha sido enviada por medios de transmisión electrónicos*.

El *Código Civil* francés describe la prueba documental como la resultante de *una sucesión de letras, de caracteres, de cifras o de cualesquiera otros signos o símbolos dotados de un significado inteligible, sean cuales fueren sus soportes y sus modalidades de transmisión*.

En el caso de Grecia, el *Código de Procedimiento civil* define los objetos de la prueba, estableciendo que sólo pueden ser *hechos reales con influencia esencial para la resolución de un juicio*.

En Irlanda, el *Código de Prueba Penal* incluye en la prueba documental *mapas, planos, gráficos, dibujos o fotografías, o, la reproducción de forma legible permanente realizada por un ordenador o a través de otros medios de información registrada de manera no legible (…)*.

En Italia, el *Código Penal* ha sido puesto al día de acuerdo con las normativas europeas y contiene un texto que define el documento electrónico como *cualquier herramienta informática que contiene información con valor probatorio o cualquier software indicado para el procesamiento de esa información*. Además, el *Código de Gobierno Electrónico* de este país, incluye la concreción de qué es un documento electrónico, la autentificación electrónica y otros conceptos como el documento de identidad electrónico o la certificación de proveedores de servicios. En particular, de acuerdo con lo establecido en este texto, un documento electrónico sería la *representación electrónica de actos, hechos o datos con relevancia jurídica* y, por otro lado, la firma electrónica queda definida como *datos en forma electrónica, unidos o asociados de forma lógica con otros datos electrónicos, usada como método de autenticación*.

En Luxemburgo, el *Código Civil* ha sido actualizado y contiene una definición para firma electrónica interpretándola como el *conjunto de datos que están vinculados a un documento legal de forma indisociable garantizando la integridad de los mismos*.

En el caso de Portugal, el *Código de Procedimiento Penal* define la prueba documental como *cualquier tipo de declaración, símbolo o nota presentada en formato escrito o en cualquier otro medio técnico de acuerdo con las leyes penales del país*, incluyendo así el documento electrónico. El *Código Civil portugués* define también la prueba documental, englobando las "reproducciones mecánicas o electrónicas de los documentos". Por último, en Portugal hemos encontrado una definición de documento electrónico en la *Ley sobre documentos y firma electrónica* que establece que es el que ha sido elaborado *a través del procesamiento electrónico de datos*.

Una referencia más directa la encontramos en el *Código sobre Policía y Prueba Penal* del Reino Unido que habla de prueba como *toda información contenida en un ordenador*. Además, el *Código sobre Abusos Informáticos* en este país cita diversas definiciones de acciones tecnológicas, como que la ejecución de un programa constituye "uso" de un ordenador, y los archivos "log" confirman que el programa ha sido ejecutado.

En el *Código de Procedimiento Penal* rumano encontramos una definición de prueba como *todo elemento fáctico que sirva para determinar, o no, la existencia de una ofensa criminal, para identificar al actor y para conocer las circunstancias necesarias para la justa resolución de un juicio*.

En Europa, ninguno de los países dispone en sus ordenamientos jurídicos de una definición concreta sobre qué es una *prueba electrónica*. En todos ellos hemos hallado referencias más o menos específicas a la prueba tradicional, englobando algunos de ellos dentro de la *prueba electrónica*.

Equivalencia de la prueba tradicional a la *prueba electrónica*

El análisis de contenido de las legislaciones muestra que la *prueba electrónica* es equivalente a la prueba tradicional en todos los países analizados. Además, hemos encontrado tres tipos de equivalencias. La primera, y más común, hace referencia a la equivalencia del documento electrónico con el documento en soporte papel. En algunas leyes se especifica el tipo de documento y se equipara también el recibo

electrónico con el recibo en soporte papel. También se equipara el contrato electrónico con el contrato en soporte papel e incluso las notificaciones realizadas de forma electrónica (fax) con las notificaciones tradicionales.

El segundo tipo de equivalencia es la referida a la equivalencia de la firma electrónica con la firma manuscrita y los actos electrónicos notariales con los actos notariales tradicionales. Por último, y como tercera categoría, se equipara el correo electrónico con el correo postal. Destaca aquí el caso de Portugal donde el correo electrónico se equipara a una conversación telefónica.

Hay un conjunto de Estados[4] que asimila expresamente los documentos electrónicos con documentos en soporte papel y les dan validez de prueba documental en un juicio. Además, hay un grupo[5] que equipara la firma electrónica con la firma tradicional, concediendo a ambas el mismo valor ante un tribunal de justicia.

Desde el punto de vista de la práctica jurídica, la gran mayoría de los jueces europeos consideran la *prueba electrónica* equivalente a la tradicional. Además, los representantes del poder judicial en Europa la consideran en su mayoría equivalente a la prueba documental. Cabe destacar aquí algunas opiniones disidentes[6] que han manifestado considerarla un soporte diferente y no un medio de prueba.

La regulación de la prueba documental en Europa juega un papel relevante a la hora de considerar la regulación de la *prueba electrónica*.

Ventajas e inconvenientes de la *prueba electrónica*

Los actores entrevistados interpretan de forma heterogénea las ventajas e inconvenientes derivados del uso de la *prueba electrónica*. Este es el caso relativo a la "fiabilidad". Mientras algunos jueces consideran que su objetividad y exactitud la hace más fiable y por lo tanto, son favorables a su utilización. Otros estiman que la falta de conocimientos para verificar su autenticidad hace que sea considerada más vulnerable y por lo tanto, menos fiable que una prueba tradicional, constituyendo un inconveniente para su uso y admisibilidad.

Entre las ventajas que los juristas y técnicos citan, aparece la apreciación de que la *prueba electrónica* ofrece una información exacta, completa, clara, precisa, veraz, objetiva y neutra. Puesto que proviene de un elemento electrónico, en el que no cabe subjetividad alguna, comparándola, por ejemplo, con las declaraciones de testigos que pueden siempre contradecirse. Además, opinan que permite disponer de una información hasta ahora imposible de obtener, como es toda aquella contenida en los artefactos electrónicos.

Otros informantes han citado como ventaja la solidez de las mismas, su fiabilidad y su viabilidad debido a la información que contiene. En varias ocasiones, se ha considerado la *prueba electrónica* como esencial para el esclarecimiento de ciertos delitos, en los que estas pruebas son el único medio probatorio existente, por lo que resulta muy útil. Otra de las ventajas en las que coinciden los jueces es la facilidad y rapidez en la obtención y el uso, así como en la conservación y almacenamiento (ventaja citada por los notarios europeos). Hemos encontrado una gran coincidencia entre todos los profesionales que opinan que el uso de documentos y firmas electrónicas favorece el desarrollo del comercio electrónico y además, abarata el coste del correo.

Los profesionales del derecho entienden como dificultad el establecimiento del valor jurídico de este tipo de pruebas, debido al desconocimiento existente sobre los procedimientos de procesado de datos y de la interpretación de las leyes procesales al respecto. Esta dificultad viene generada por la falta de una regulación propia y sistemática, así como por la falta de jurisprudencia homogénea. Además, estos profesionales muestran un temor a la vulnerabilidad y facilidad con que estas pruebas pueden ser manipuladas, dado su alto grado de volatilidad, lo que resulta uno de los principales inconvenientes a la hora de probar su autenticidad. Algunos opinan que se trata de pruebas muy técnicas que son desconocidas para jueces y fiscales y que resultan difíciles de explicar, de ahí el rechazo a su admisión en juicio. Como inconvenientes, se citan también las dificultades para la preservación de la prueba electrónica y la escasa información sobre cómo almacenarla correctamente para su conservación

Los inconvenientes citados por los expertos informáticos, tanto del sector público como del privado, hacen referencia a la falta de soporte legal y de modelos de certificación. Manifiestan que son más difíciles de aceptar en los tribunales, debido a que los jueces piden más garantías que con otras pruebas tradicionales. Los expertos interpretan como un inconveniente la incomprensión que muestran algunos órganos judiciales en Europa sobre las tareas que desarrollan. Además, estos expertos consideran que el proceso de obtención e interpretación de la información proporcionada por un dispositivo electrónico para convertirla en una *prueba electrónica,* requiere mucho tiempo, lo que conlleva un alto coste y dificulta su utilización.

[4] Alemania, Bélgica, España, Finlandia, Francia, Irlanda, Italia, Luxemburgo, Portugal y Rumania.

[5] Bélgica, España, Finlandia, Francia, Holanda, Italia, Luxemburgo, Portugal y Rumania.

[6] Fiscales de Portugal, y España. Rumania: no es un tipo de prueba diferente porque no está establecido por ley.

Las ventajas que ofrece la *prueba electrónica* en Europa, consisten principalmente en permitir la obtención de una información completa, veraz y hasta ahora imposible de obtener. Como desventajas se encuentran la alta especialización de los conocimientos técnicos necesarios para poder presentarla ante los tribunales, así como el coste en tiempo y dinero que supone su obtención.

VENTAJAS:

INFORMACIÓN: EXACTA, COMPLETA, CLARA, PRECISA, VERAZ, OBJETIVA, NOVEDOSA Y NEUTRA.

PRUEBA: SÓLIDA, ÚTIL, FIABLE, VIABLE, ESENCIAL PARA PROBAR CIERTOS DELITOS QUE ANTES NO SE PODÍAN PROBAR.

FÁCIL: OBTENCIÓN, USO, CONSERVACIÓN Y ALMACENAMIENTO.

LOS DOCUMENTOS ELECTRÓNICOS JUNTO CON LA FIRMA ELECTRÓNICA FACILITAN EL COMERCIO ELECTRÓNICO SIENDO MÁS RÁPIDO Y SEGURO.

INCONVENIENTES:

- ESCASA/FALTA REGULACIÓN PROPIA Y SISTEMÁTICA.
- ESCASA JURISPRUDENCIA.
- MATERIA DESCONOCIDA Y MUY TÉCNICA. POCOS EXPERTOS.
- EXIGE CONOCIMIENTOS ESPECÍFICOS.
- DIFÍCIL DE PRESENTAR AL TRIBUNAL DE FORMA COMPRENSIBLE.
- MÁS DIFÍCILES DE SER ACEPTADAS EN LOS TRIBUNALES: LOS JUECES PIDEN MÁS GARANTÍAS QUE CON OTRAS PRUEBAS.
- FALTA DE INFRAESTRUCTURA TÉCNICA EN LAS DEPENDENCIAS JUDICIALES.
- ALTO COSTE PARA EXAMINAR E INTERPRETAR LA INFORMACIÓN.
- DIFÍCIL CONOCER CÓMO SE PROCESAN LOS DATOS Y CÓMO SE INTERPRETAN LAS LEYES PROCESALES ESPECÍFICAS.
- DIFÍCIL PROBAR LA AUTENTICIDAD, INTEGRIDAD, FIABILIDAD Y EL ORIGEN DE LOS DATOS.
- VOLATILIDAD DE LOS DATOS Y FÁCIL MANIPULACIÓN.
- DIFÍCIL IDENTIFICACIÓN DEL AUTOR DEL DELITO.
- DIFÍCIL DE CONSERVAR, PRESERVAR Y ALMACENAR.
- DIFÍCIL ESTABLECER EL VALOR JURÍDICO DE LA PRUEBA.
- FALTA DE SOPORTE LEGAL Y MODELOS DE CERTIFICACIÓN.

B) SOBRE LA LEY Y LA JURISPRUDENCIA

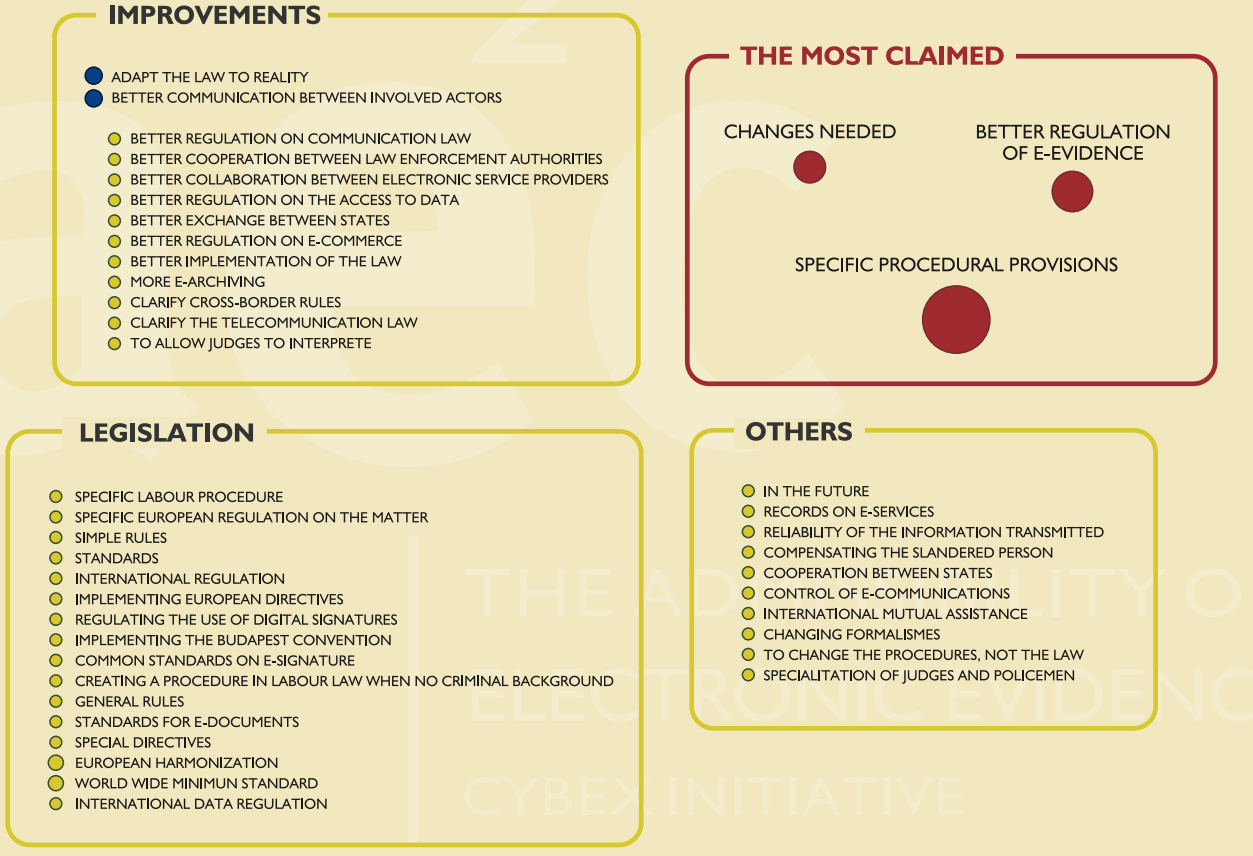
El marco legal regulador de la *prueba electrónica* en Europa se compone fundamentalmente de una serie de normas de procedimiento, textos de derecho civil, penal y comercial, disposiciones sobre comercio electrónico o sobre firma electrónica, entre las que no hemos encontrado una regulación específica para la *prueba electrónica*.

La interpretación analógica de las disposiciones contenidas en estos textos para la prueba tradicional regulan también las *pruebas electrónicas* en Europa.

La regulación de la *prueba electrónica* la hemos encontrado esencialmente en las siguientes jurisdicciones: la regulación del derecho civil y regulación del derecho penal, seguidos de la regulación de la prueba en el derecho laboral y de la regulación que de la misma se hace en otras materias legales[7].

La percepción subjetiva de los juristas sobre la regulación de la *prueba electrónica* (Gráfico 1) es heterogénea y además presenta múltiples contradicciones. La tendencia principal entre abogados, fiscales y notarios es la de considerar que la *prueba electrónica* se encuentra actualmente bien regulada.

GRÁFICO 1: CAMBIOS LEGISLATIVOS PREFERIDOS POR LOS JURISTAS



Fuente de datos y elaboración propias.

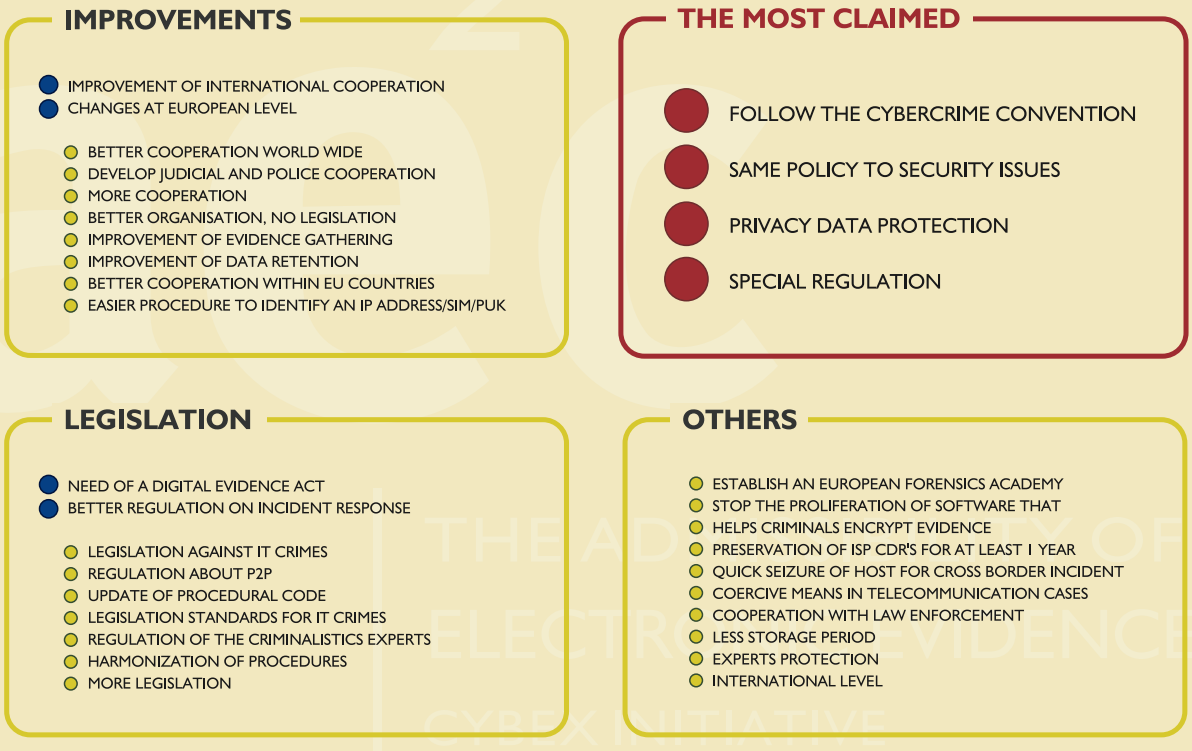
[7] Normativa administrativa, comercial, leyes sobre la organización judicial y normas Constitucionales.

Sin embargo, los jueces, que son los que tienen que interpretar la ley debido a la laguna legal, se muestran divididos en sus opiniones de acuerdo con su especialidad, pero la opinión mayoritaria favorece a quienes se inclinan a pensar que la situación legal actual no es la idónea y necesita cambios para adaptar las leyes a la realidad tecnológica.

Los que se muestran favorables a la introducción de cambios en la actual situación legal, se decantan principalmente por cambios que aporten una regulación específica de las distintas dimensiones de la *prueba electrónica* y preceptos de procedimiento específicos a nivel nacional. Por otro lado, a nivel europeo, los juristas prefieren una armonización (de la materia), pero apostillan que ha de hacerse a través de normas generales que permitan a cada país su implementación de acuerdo con su tradición jurídica. Por último, están quienes opinan que a nivel internacional, debería haber una norma de mínimos.

La percepción subjetiva que tienen los expertos en informática forense sobre la situación legal y jurisprudencial (Gráfico 2), es bastante equilibrada. Sin embargo la mayoría de estos expertos[8] opinan que la situación es mejorable. Los cambios más significativos que introducirían, consisten en establecer una política de seguridad común, seguir la regulación de la Convención sobre Cibercrimen del Consejo de Europa, establecer una regulación específica para la *prueba electrónica* y mejorar la protección de datos personales.

GRÁFICO 2: CAMBIOS LEGISLATIVOS PREFERIDOS POR LOS EXPERTOS EN INFORMÁTICA FORENSE



Fuente de datos y elaboración propias.

[8] Expertos de Austria, Alemania, Irlanda, Reino Unido y Francia consideran que la situación legal y jurisprudencial es la adecuada. La situación sería mejorable para los expertos de Bélgica, Grecia, España, Dinamarca, Portugal y Rumania. En Italia y Holanda las opiniones son contradictorias, a favor y en contra dentro del mismo país. El experto de Luxemburgo no opina.

Las interpretaciones de los expertos legales y los expertos en informática forense sobre la situación actual de la admisibilidad de la *prueba electrónica* ante los tribunales, coinciden en que hay una necesidad de desarrollar preceptos específicos que contribuyan a aportar seguridad jurídica. También comparten la necesidad de desarrollar unas normas europeas que garanticen una homogeneidad mínima en el tratamiento de la *prueba electrónica*, así como de establecer unas normas internacionales que ayuden a mejorar la cooperación internacional.

Conveniencia de un marco europeo que regule la *prueba electrónica*

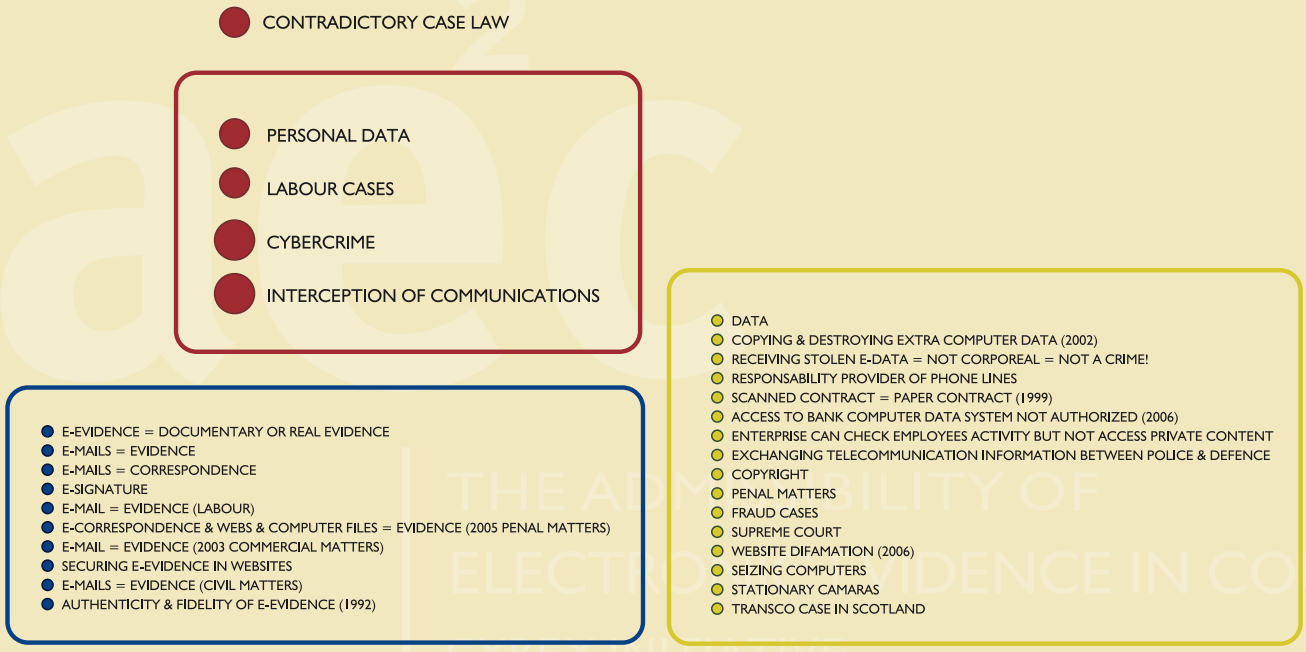
La gran mayoría de juristas europeos considera conveniente la posibilidad de algún tipo de regulación de las diferentes dimensiones de la *prueba electrónica* desde Europa. Las argumentaciones son diversas. Hemos encontrado opiniones compartidas, como que el marco europeo es necesario debido a la dimensión transnacional de los delitos que las *pruebas electrónicas* tratan de probar, a la vez que facilitaría la cooperación internacional. También facilitaría una mayor uniformidad en el desarrollo de la *prueba electrónica*, citando como ejemplos de acciones necesarias la armonización en la protección de datos y los procedimientos de recogida de *pruebas electrónicas*. Otro grupo menos numeroso de juristas considera que la regulación de la *prueba electrónica* debe seguir siendo exclusiva de los Estados. Los representantes de Austria, Dinamarca y Finlandia consideran que la regulación nacional es suficiente ya que da cobertura a todos los aspectos de la prueba, incluida la electrónica. Por otro lado, es necesario señalar las opiniones de los representantes judiciales griegos, quienes consideran que sin una norma europea común, la adecuación de la legislación actual a la realidad tecnológica no será posible en su país.

Un marco normativo europeo que regule la *prueba electrónica* es visto como un elemento positivo para la evolución legislativa de la materia.

Jurisprudencia existente

Los casos de jurisprudencia actuales más relevantes hacen referencia al cybercrimen, intercepción de las comunicaciones,

GRÁFICO 3: CASOS MÁS FRECUENTES DONDE LA PRUEBA ELECTRÓNICA ES UTILIZADA



Fuente de datos y elaboración propias.

casos de derecho laboral y a la vulneración de la protección de datos (Gráfico 3).

Algunos juristas han resaltado la existencia de casos de jurisprudencia contradictoria que revelan una falta de homogeneidad en los criterios de admisibilidad de las *pruebas electrónicas.* En casos muy similares, en unas ocasiones las *pruebas electrónicas* han sido admitidas y en otras han sido rechazadas.

Los expertos en informática forense del sector público trabajan principalmente en casos de cibercrimen, cibercterrorismo, pornografía infantil y delitos económicos cometidos a través de medios electrónicos. Los expertos del sector privado trabajan con mayor frecuencia en casos de abuso de medios corporativos, investigación en aparatos tecnológicos (GSM y SIM *forensics*, recuperación de datos de GPS), incidentes de seguridad, delitos económicos y de propiedad intelectual. Los empresarios se enfrentan a problemas en el medio laboral referidos habitualmente a casos de uso incorrecto y abuso de los recursos corporativos electrónicos, así como a problemas de seguridad de los datos y de los ordenadores. También, citan fraudes bancarios y delitos sobre propiedad intelectual, además de los derivados del comercio electrónico. No obstante, la mayoría de estos empresarios no dispone de un protocolo que regule el uso del material informático puesto a disposición de sus trabajadores. Tampoco disponen de una infraestructura que les aconseje sobre cómo protegerse de este tipo de delitos.

C) SOBRE EL PROCEDIMIENTO PARA LA OBTENCIÓN, CONSERVACIÓN Y PRESENTACIÓN DE LA *PRUEBA ELECTRÓNICA* ANTE LOS TRIBUNALES

Las normas de procedimiento no recogen procedimiento específico alguno que regule la obtención, conservación y presentación de la *prueba electrónica* ante los tribunales de justicia. En general, los países aplican por "analogía" la regulación del procedimiento general de la prueba tradicional.

Casi la mitad de las normas analizadas (48%) contemplan procedimientos procesales que son de aplicación analógica a la *prueba electrónica*. Las normas más similares a lo que sería un procedimiento para la *prueba electrónica* las hemos encontrado en Reino Unido y Bélgica. El *Código sobre la Policía y la Prueba Penal*[9] vigente en Reino Unido regula de manera específica la obtención de "pruebas de ordenadores", y en la *Ley relativa a los Delitos Informáticos* belga se incluyen preceptos sobre la recogida de las pruebas que son aplicables a las *pruebas electrónicas*.

Otros procedimientos que pueden ser utilizados por analogía a la *prueba electrónica* son los contemplados en las leyes procesales en Europa, desarrollados para la interceptación de las comunicaciones o telecomunicaciones, y de las normas procesales a seguir cuando existe posibilidad de infringir los derechos fundamentales de la persona.

La percepción de los juristas sobre la existencia o no de un procedimiento es sesgada debido a cómo se interprete el concepto "procedimiento". Unos consideran que la aplicación analógica hace que las normas de procedimiento para la prueba tradicional se apliquen a la *prueba electrónica* y por lo tanto, en su opinión, existe un único procedimiento para todas las pruebas. Otros han interpretado el concepto "procedimiento" de manera más restringida y consideran que no existe un procedimiento concreto para la *prueba electrónica,* o que sólo hay preceptos que regulan algún aspecto de la obtención, conservación y presentación de este tipo de pruebas. Por ejemplo, este es el caso del procedimiento a seguir en materia penal para monitorizar e interceptar las comunicaciones. Procedimiento que consiste en la exigencia de petición al juez de una orden judicial. Esta orden judicial es necesaria también para llevar a cabo una investigación, o para la obtención de pruebas o *pruebas electrónicas* en los supuestos donde pueda haber una vulneración de derechos fundamentales.

Los notarios, de forma unánime, opinan que no disponen de ningún procedimiento específico para la custodia de las *pruebas electrónicas* y los procedimientos a los que se refieren son los de creación de firmas electrónicas. En Italia

[9] Police and Criminal Evidence Act, PACE.

los notarios pueden utilizar procedimientos informales para archivar documentos electrónicos, cuyo cumplimiento no es obligatorio.

La policía y los expertos privados en informática forense no cuentan con un procedimiento específico para la obtención, conservación y presentación de la *prueba electrónica* ante los tribunales, salvo en Austria y Rumania. En estos países sí existe un procedimiento para la obtención[10]. En Reino Unido[11] y Rumania[12] siguen las reglas internas de la policía como procedimiento. En Luxemburgo, la policía está trabajando en un procedimiento interno de obtención y análisis de *pruebas electrónicas*. En Finlandia se está elaborando una estrategia de investigación criminal de IT, que se puede llegar a convertir en un manual de procedimiento.

Desde el punto de vista de la práctica legal, los juristas coinciden en que en Europa existen normas de procedimiento general que regulan la obtención de la prueba en materia penal y comercial en algunos casos (Finlandia), que son extensibles a las *pruebas electrónicas* por analogía, pero no en el resto de jurisdicciones. Hacen referencia también a que no hay un procedimiento establecido para la conservación o preservación de la *prueba electrónica* y que la presentación de la misma, ante los tribunales, se hará en cada país como resulte de la interpretación analógica de los preceptos establecidos para la prueba tradicional, esto es, como prueba documental y como prueba testifical en la mayoría de los casos.

En el sistema normativo procesal vigente en Europa no existen procedimientos específicos que regulen la obtención de la *prueba electrónica* salvo en los preceptos legislativos de dos países, Reino Unido y Bélgica. Preceptos que son relativos a la obtención de pruebas de ordenadores. En ninguno de los países europeos no hemos encontrado procedimiento alguno para la preservación y presentación de la *prueba electrónica* ante los tribunales.

D) SOBRE LA ADMISIBILIDAD DE LA *PRUEBA ELECTRÓNICA*

Autoridad competente para la admisibilidad de las *pruebas electrónicas*, motivación de la exclusión y custodia de las mismas

La figura del juez o del tribunal se ha revelado como la máxima autoridad competente para decidir sobre la admisibilidad o no de una *prueba electrónica* en Europa, siguiendo tanto el resultado del análisis de las legislaciones como de las preguntas formuladas a los juristas. En algunos países, como Grecia y Luxemburgo, además de las menciones al juez, hemos encontrado referencias particulares a la figura del fiscal general como autoridad competente.

La admisibilidad está muy relacionada con la posibilidad, o no, de exclusión de la *prueba electrónica* sin motivación previa. Podemos afirmar que ninguna de las normas analizadas permite, ni tampoco entrevistado alguno acepta, la posibilidad de excluir una *prueba electrónica* sin la debida motivación por parte del órgano judicial. Sin embargo, los jueces comerciales daneses puntualizan que la motivación en algunos casos de la exclusión de la prueba y de la *prueba electrónica* puede realizarse de manera muy breve y de forma verbal durante la audiencia.

Durante la investigación, son los agentes de la policía y los fiscales los encargados de custodiar la *prueba electrónica* en los procedimientos penales. Durante la fase de juicio, es el órgano judicial el encargado de la custodia de estas pruebas (concretamente, la figura del secretario judicial en la mayoría de los países). En materia civil, son principalmente las partes quienes custodian las pruebas que serán presentadas ante el juez o tribunal cuando éste así lo requiera, tanto en la fase previa al juicio como durante el mismo. En algunos países los notarios y expertos son los encargados de guardar y hacer llegar al tribunal en su caso las *pruebas electrónicas*.

Requisitos que ha de cumplir la *prueba electrónica* para ser admitida ante los tribunales

En Europa, de acuerdo con los textos legales, coexisten dos modelos de países respecto a los requisitos que deben reunir las pruebas para ser admitidos en juicio. Un grupo de países tiene en común que su tradición jurídica establece unos criterios muy amplios de admisibilidad de la prueba. Se basan en la libre consideración del juez a la hora de admitir o no la *prueba electrónica* (Austria, Dinamarca, Suecia, Finlandia). El

[10] En Rumania, los "G8 Proposed Principles for the Procedures Relating to Digital Evidence" no son obligatorios ni de seguimiento recomendado.

[11] Association of Chef Police Officers.

[12] Directrices: Operacional procedure to be followed for search of computers.

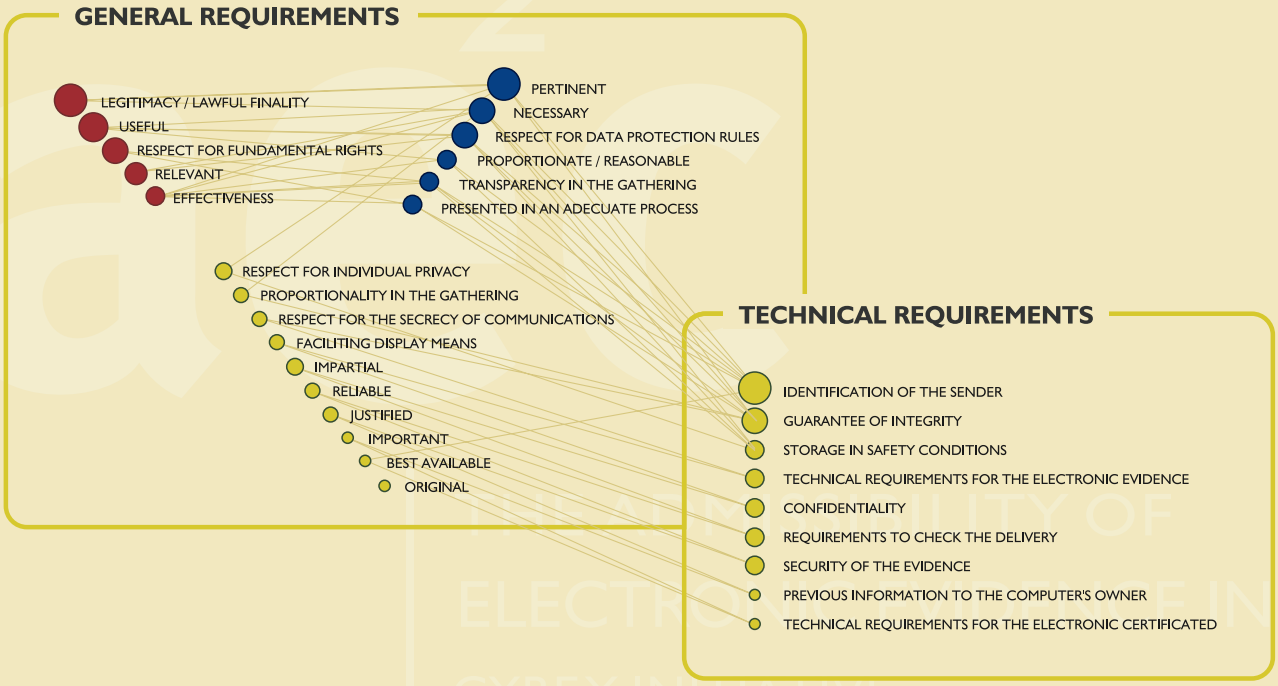
otro conjunto de países comparte que sus legislaciones regulan de manera más restrictiva la admisibilidad de la prueba de acuerdo a una serie de requisitos, de la prueba o los medios de prueba, establecidos por ley.

La legalidad de la prueba[13] es el requisito que se cita con más frecuencia en las leyes (Gráfico 4). En algunos países, como Alemania, Irlanda y Reino Unido, no se aplica la doctrina de la fruta del árbol envenenado[14], por ello que el requisito de la legalidad no siempre resulta de aplicación.

Otro requisito contemplado en las leyes es el respeto por los derechos fundamentales[15], entre éstos es frecuente encontrar menciones al respeto de las normas sobre protección de datos personales y los derechos de los trabajadores. La fiabilidad de la prueba, junto con su pertinencia, y que sea la mejor disponible en un determinado momento, son otros de los requisitos fundamentales que el juez examinará para decidir sobre la admisibilidad de una prueba determinada.

Otro de los requisitos recogidos a lo largo de las legislaciones y cuyo respeto marcará la admisibilidad o no de la *prueba electrónica* son la utilidad, proporcionalidad y efectividad de la misma. Entendiendo la efectividad como la capacidad para probar la alegación.

GRÁFICO 4: REQUISITOS LEGALES DE LA PRUEBA ELECTRÓNICA PARA SER ADMITIDA EN JUICIO



Fuente de datos y elaboración propias.

[13] Código civil italiano. Código de procedimiento penal alemán, belga, irlandés, portugués, rumano. Leyes de procedimiento civil en España, Francia, Grecia, Holanda, Luxemburgo, entre otros ejemplos.

[14] Esta doctrina establece el carácter ilícito de las pruebas obtenidas de un procedimiento que se demuestre viciado, quedando éstas contaminadas por la ilegalidad del procedimiento.

[15] Ley de procedimiento danesa. Ley de procedimiento civil en España, en Luxemburgo. Código de procedimiento penal alemán y portugués, entre otros ejemplos.

Finalmente, algunas leyes establecen como requisito que la prueba sea original siempre que sea posible, y no una copia. Además de la originalidad, la prueba ha de ser directa y no de oídas o indirecta, (conocida como *hearsay*). Estas son reglas de exclusión que rigen la admisibilidad de la *prueba electrónica* en Reino Unido e Irlanda.

Si bien los requisitos citados anteriormente aparecen en los textos legales, en la práctica judicial no siempre se cumplen por todas las partes. Hemos querido saber cuáles son los requisitos que se incumplen con mayor frecuencia en el ámbito jurídico europeo. La opinión subjetiva de los juristas muestra que es el respeto por los derechos fundamentales, especialmente los relativos al derecho a la protección de datos y los derechos de los trabajadores los que se incumplen con mayor frecuencia a la hora de presentar una *prueba electrónica* ante los tribunales. Esto hace que estas pruebas sean rechazadas a menudo. Los requisitos técnicos formales que se incumplen más habitualmente en Europa son los relativos al cumplimiento de las medidas necesarias para la comprobación de la autenticidad y la inalterabilidad del documento electrónico, del correo electrónico enviado así como la falta de firma electrónica en documentos que quedan sin fuerza probatoria a la hora de ser presentados ante los tribunales. Además, en muchas ocasiones, la cadena de custodia es vulnerada generando inseguridad jurídica en la *prueba electrónica* presentada.

Influencia del respeto de las garantías de legalidad

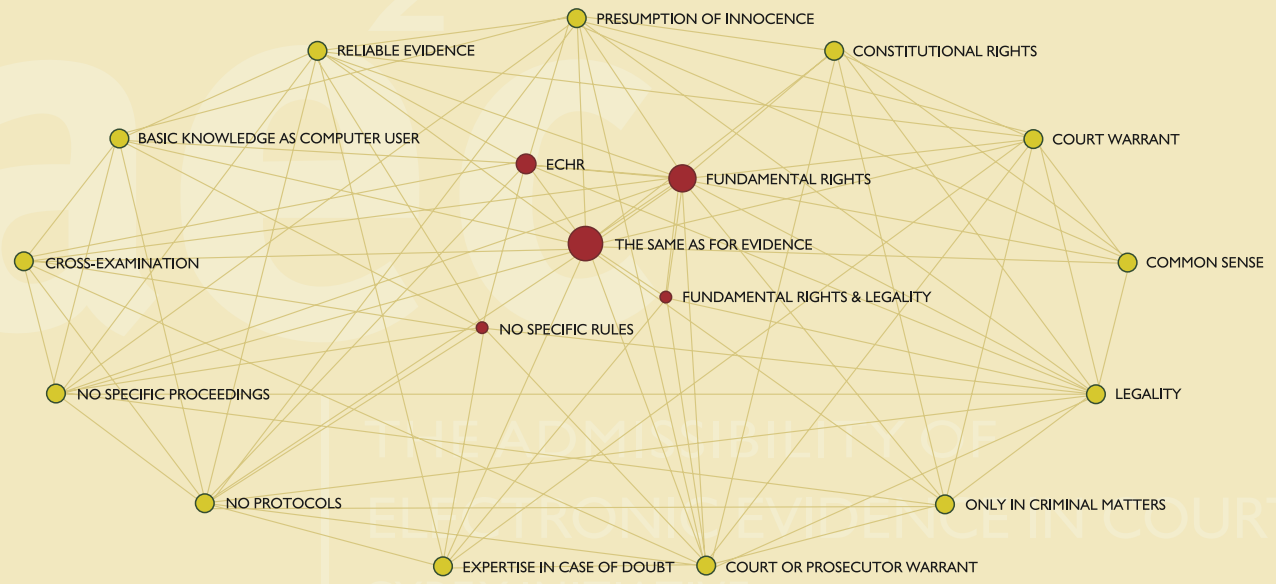
a) En la admisibilidad de la *prueba electrónica*

El respeto de las garantías de legalidad es uno de los requisitos exigidos en la mayoría de las legislaciones. En la práctica, el conjunto de los magistrados coincide en que el respeto de estas garantías de legalidad influye positivamente sobre la admisibilidad de la *prueba electrónica*. Otros profesionales de la justicia indican que lo relevante es que sea un juicio justo u obtener la verdad material (Dinamarca y Finlandia). En Dinamarca se puntualiza también que dichas garantías sólo tendrán influencia si una de las partes objeta sobre el respeto de las garantías de legalidad.

b) En el proceso de obtención, análisis y presentación de la *prueba electrónica* en juicio

Respecto a las garantías de legalidad que se deben tener en cuenta en el proceso de obtención, análisis y presentación de

GRÁFICO 5: PERCEPCIÓN DE LAS GARANTÍAS DE LEGALIDAD QUE CONSIDERAN LOS JURISTAS QUE DEBEN SER RESPETADAS



Fuente de datos y elaboración propias.

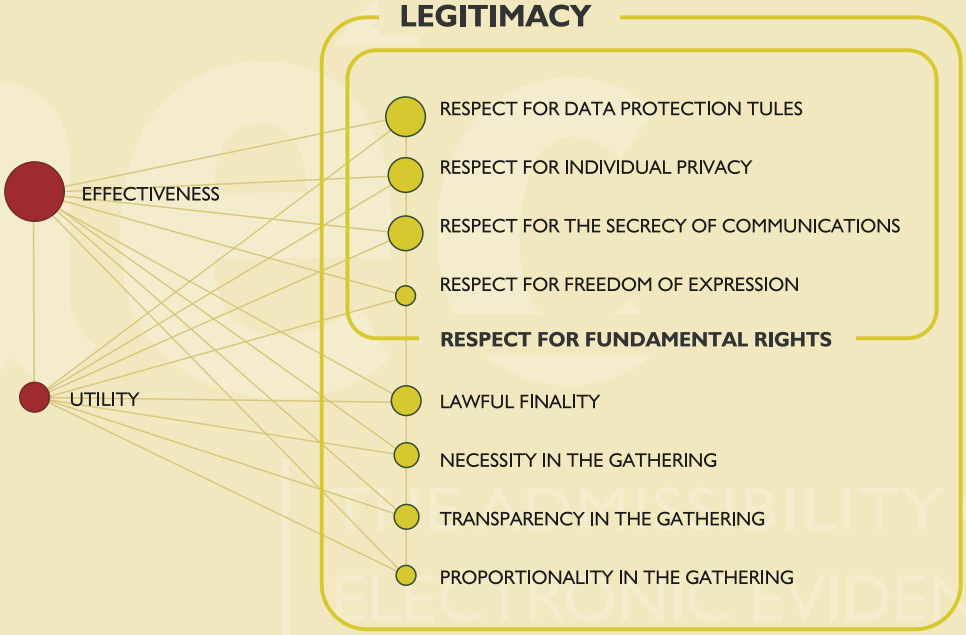
la *prueba electrónica* en juicio, buena parte de las opiniones vertidas por los juristas europeos señalan la falta de normas específicas relativas (Gráfico 5). Por lo que se declaran a favor del mismo tipo de medidas que se deben respetar para cualquier otro tipo de prueba. Las menciones positivas insisten en el respeto por los derechos fundamentales y por la jurisprudencia proveniente del Tribunal Europeo de Derechos Humanos, así como por el respeto de la legalidad.

Principios que afectan la admisibilidad de la *prueba electrónica*

Los principios relativos a la eficacia, utilidad y legitimidad de la *prueba electrónica* ocupan un papel relevante en las diferentes legislaciones europeas. La necesidad de obtención de la prueba, la transparencia durante la obtención y el respeto por la libertad de expresión son principios reflejados en las normas, pero ocupan una posición secundaria en lo que a admisibilidad de la prueba se refiere. Los principios que afectan de manera concreta a la *prueba electrónica* y tienen por tanto mayor relevancia, son el respeto por las normas de protección de datos, el respeto por el secreto de las comunicaciones y el respeto por el derecho de libertad de expresión (Gráfico 6).

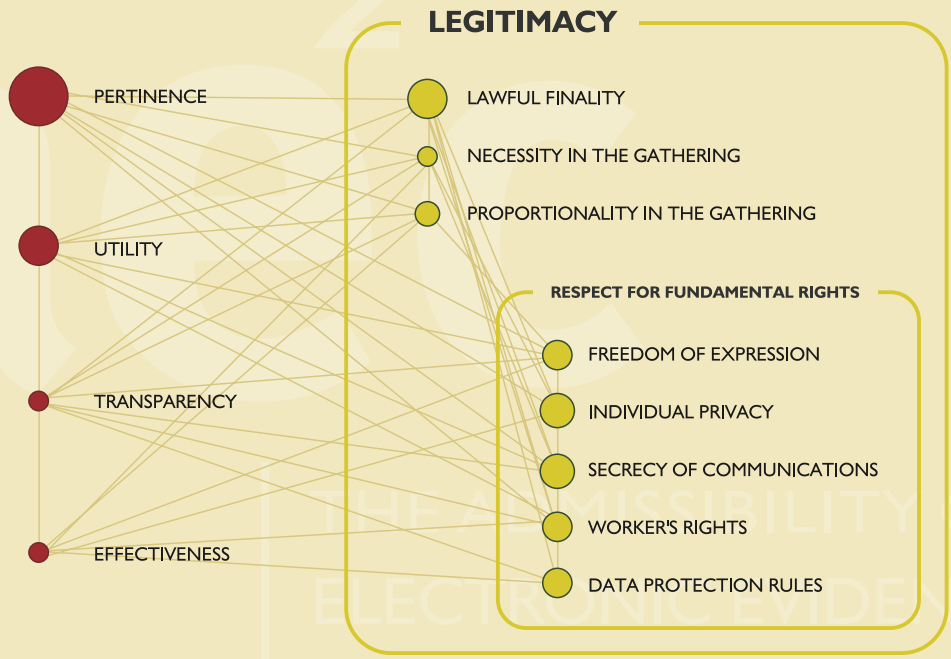
En la práctica, mientras que los juristas europeos consideran que son los principios de legitimidad (destacando la posición privilegiada como parte integrante de este principio, del respeto por los derechos fundamentales, la pertinencia de la prueba y utilidad de la misma tienen mayor influencia. Los técnicos expertos en Informática forense destacan que actúan teniendo en cuenta el respeto por los derechos individuales. Además citan el respeto por las normas de protección de datos (Alemania y Grecia), el mantenimiento de la confidencialidad (Francia, Luxemburgo e Irlanda), el desarrollo de sus funciones mediante material encriptado como principios básicos (Italia y Reino Unido). Además, señalan que cuentan con el soporte legal de un notario (España), así como con la presencia de testigos (España y Rumania) (Gráfico 7).

GRÁFICO 6: PRINCIPIOS LEGALES ENCONTRADOS EN LAS LEGISLACIONES QUE CONDICIONAN LA ADMISIÓN DE LA PRUEBA



Fuente de datos y elaboración propias.

GRÁFICO 7: PERCEPCIÓN DE LOS JURISTAS SOBRE LOS PRINCIPIOS QUE AFECTAN A LA ADMISIBILIDAD DE LAS PRUEBAS ELECTRÓNICAS



Fuente de datos y elaboración propias.

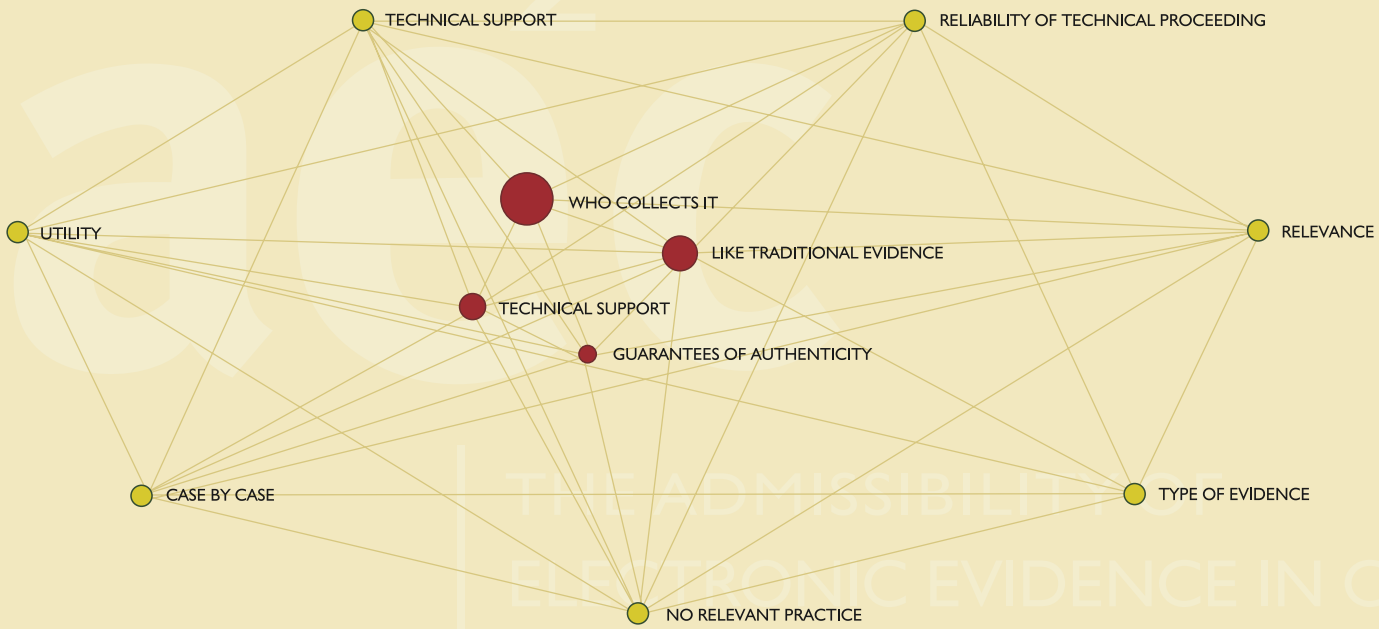
Factores que influyen en el valor probatorio de la *prueba electrónica*

El respeto por la legalidad en la obtención de la prueba tiene un papel fundamental a la hora de valorar la admisibilidad de la misma. Por esta razón, hemos querido conocer quiénes son los responsables de obtener la prueba, tanto la tradicional como electrónica de acuerdo con las leyes. Por un lado, el órgano judicial, en las figuras del juez o del tribunal y del fiscal en colaboración con la policía, tienen un papel fundamental para la obtención de las pruebas en Europa. Por otro lado, la legislación otorga a las partes la responsabilidad de la obtención de la prueba en materia civil. La figura del experto, también se cita como agente responsable de la obtención de la *prueba electrónica* tanto en materia civil como en materia penal.

La afirmación anterior adquiere gran relevancia al conocer que, de acuerdo con las opiniones de los juristas, la persona encargada de la obtención de la *prueba electrónica* es el factor que más influye en el valor probatorio que se le pueda atribuir. Lo que indica que, el hecho de que sea la policía la encargada de obtener la *prueba electrónica,* al contar con el soporte del órgano judicial, se valora de manera relevante a la hora de admitir o no una prueba. El soporte técnico por un lado y las garantías de autenticidad por otro, completan el cuadro de factores que más influyen en los órganos juzgadores europeos a la hora de conceder mayor o menor valor probatorio a una determinada prueba. Otro grupo de magistrados no considera que exista un factor relevante, sino que son los mismos que han de tenerse en cuenta para la prueba tradicional (Gráfico 8).

Estas afirmaciones demuestran el grado de interés y preocupación por la autenticidad e integridad de este tipo de pruebas compartido por el colectivo judicial europeo.

GRÁFICO 8: PERCEPCIÓN DE LOS JURISTAS DE LOS FACTORES QUE DAN MÁS VALOR PROBATORIO A LA PRUEBA ELECTRÓNICA



Fuente de datos y elaboración propias.

E) SOBRE LOS EXPERTOS EN INFORMÁTICA FORENSE

Formación y requisitos necesarios para trabajar como experto en informática forense en Europa

En Europa hay una ausencia de normas que determinen las características que tiene que reunir un experto en informática forense. Careciendo de preceptos legales, lo que más valoran, tanto juristas como técnicos es la experiencia específica.

La formación básica que los expertos consideran necesaria para considerarse ellos mismos expertos en informática forense, debería de ser como mínimo una licenciatura. Preferiblemente, si la licenciatura es en informática, ingeniería o matemáticas. Además, consideran esencial una formación continua y especializada como el único medio de mantenerse actualizados. También sabemos que la policía especializada recibe formación interna de organismos públicos, nacionales e internacionales y de compañías privadas. Sin embargo, no hemos encontrado que haya una formación universitaria reglada en materia de análisis forense de medios digitales, mientras que sí existen formaciones de postgrado en informática forense (Francia) y en investigación de cibercrímenes (Irlanda). En Europa conviven expertos en informática forense privados con los de los cuerpos y fuerzas de seguridad del Estado. Sólo en Rumania, para actuar como experto se ha de contar con la autorización o certificación del Estado.

La gran mayoría de profesionales del derecho considera que las leyes no especifican requisitos especiales para actuar como experto en informática forense ante un tribunal. Citan como fundamental el requisito formal de estar inscrito en las listas de expertos de las que disponen los tribunales en Europa. Son menos las opiniones que citan que el requisito a cumplir es el de ser "experto en informática".

Percepciones de los expertos en informática forense vistos por los juristas europeos y por los expertos consultados

Los juristas europeos identifican principalmente que son los policías o los fiscales quienes deberían ser los expertos en informática forense. Además, creen que estos profesionales deberían tener una certificación en análisis forense expedido por el sector privado. La opinión de los expertos está muy dividida. Los expertos prefieren, considerando la ausencia de titulación específica, que tengan por lo menos cinco años o más de experiencia profesional. Respecto a las profesiones que consideran más adecuadas para ser expertos se encuentran los abogados y los policías.

GUÍA DE MEJORA

Las fuentes que inspiran la presente guía de mejora están basadas en las percepciones y visiones subjetivas de los profesionales: juristas, técnicos y empresarios en Europa.

- Respecto a la **regulación** de la *prueba electrónica*, **los juristas** consideran que a nivel nacional existe una necesidad de realizar cambios en el cuerpo legislativo actual que contribuyan a disminuir el grado de inseguridad legislativa. Abogan por una mejor regulación nacional de la *prueba electrónica*, concretamente del procedimiento, que permita la obtención, preservación y presentación de estas pruebas cumpliendo todas las garantías legales específicas/propias para que puedan ser admitidas en juicio como una tipología más de prueba. A nivel europeo e internacional expresan la necesidad de desarrollar una serie de directrices de mínimos en materia de procedimiento, que aseguren la buena cooperación entre Estados en cuanto a la obtención y preservación. La cooperación internacional resulta esencial para lograr una mayor efectividad en la lucha individual de cada país contra los delitos cometidos a través de/o en medios digitales, que debido a su naturaleza, en muchas ocasiones son transnacionales.

  Los cambios que **los expertos en informática forense**, tanto del sector público como del sector privado, consideran necesario llevar a cabo, se refieren en primer lugar a que la *prueba electrónica* disponga de una regulación específica a nivel nacional. Otros, recomiendan su regulación a través de la implementación de protocolos que desarrollen la protección de los derechos fundamentales en las fases de obtención, preservación y presentación de la *prueba electrónica,* para así poder mejorar el cumplimiento de las garantías de admisibilidad de este tipo de pruebas. Al igual que los juristas consideran que es necesario realizar cambios a nivel europeo, dictando unas normas mínimas de actuación. Específicamente, consideran de gran importancia que los países cumplan las disposiciones contenidas en la Convención de Budapest sobre Cybercrimen del Consejo de Europa. Además creen que sería conveniente actuar a nivel internacional para lograr una mejora en la cooperación entre Estados en materia de obtención y preservación.

SOBRE LA REGULACIÓN DE LA *PRUEBA ELECTRÓNICA:*

- REGULACIÓN ESPECÍFICA TANTO A NIVEL NACIONAL COMO EUROPEO QUE APORTE SEGURIDAD JURÍDICA.
- NORMATIVA EUROPEA QUE GARANTICE LA HOMOGENEIDAD EN EL TRATAMIENTO DE LAS MISMAS.
- NORMAS INTERNACIONALES QUE CONTRIBUYAN A MEJORAR LA COOPERACIÓN INTERNACIONAL.

- Respecto al **ejercicio profesional en informática forense**, tanto **los juristas como los expertos** coinciden en que para el ejercicio de la profesión, la experiencia es la característica relevante a la que confieren un gran valor tanto en el presente como en sus visiones de futuro. Ambos opinan que el perfil que debiera reunir un profesional en informática forense es el que resulta de ser licenciado en informática, ingeniería o matemática. Además, los expertos consideran necesario disponer de un certificado en análisis forense de medios digitales expedido por una autoridad pública, y contar con, como mínimo, dos años de experiencia si se dispone de título universitario. Para quienes no tengan formación universitaria opinan que, como mínimo, deberían tener cinco años de experiencia específica y hacen hincapié en la necesidad de la formación continuada. Por su parte, los juristas consideran que un profesional debe ser miembro de la policía y disponer de un certificado en análisis forense de medios digitales privado.

PROFESIONALES EN INFORMÁTICA FORENSE: Requisitos deseables

- EXPERIENCIA RELEVANTE EN ANÁLISIS FORENSE DE MEDIOS DIGITALES.
- LICENCIATURA EN INGENIERÍA.
- FORMACIÓN CONTINUADA.

- **Los empresarios y organizaciones profesionales** en Europa aluden principalmente a tres grandes temas: prevención, formación y legislación. Referente a la prevención, defienden la necesidad de crear protocolos informáticos estándares para uso de los empresarios en las relaciones laborales. En cuanto a formación, estiman conveniente que debieran ponerse en marcha iniciativas de asesoramiento. Medidas que les permitan conocer cómo proceder en la recogida y almacenamiento de *pruebas electrónicas* para no disminuir su valor probatorio ante los tribunales. También, abogan por la utilidad del intercambio de buenas prácticas entre países. Respecto a la legislación, expresan la necesidad de reformar y clarificar la legislación existente en materia de *prueba electrónica*. Específicamente, proponen incrementar la seguridad de las comunicaciones electrónicas, la implementación efectiva de la firma electrónica y la reducción del tiempo de almacenamiento de los documentos. Sin embargo otros, de determinados países europeos, donde rige el principio de la libre admisibilidad de la *prueba electrónica,* insisten en que la situación legal y jurisprudencial es adecuada y que no es necesaria ninguna modificación de la legislación.

ACCIONES DE CAMBIO SUGERIDAS POR LOS EMPRESARIOS EUROPEOS:

- PREVENCIÓN: PROTOCOLOS INFORMÁTICOS.
- FORMACIÓN: ASESORAMIENTO SOBRE PROCEDIMIENTO DE RECOGIDA Y ALMACENAMIENTO.
- LEGISLACIÓN: REFORMA Y CLARIFICACIÓN DE LA NORMATIVA EXISTENTE.

- Unos consideran que el futuro de la *prueba electrónica* pasa por una regulación específica de la misma a nivel tanto nacional como europeo, que asegure el desarrollo progresivo de la materia adaptando, de manera adecuada, la legislación a las nuevas realidades sociales existentes. Mientras que otros visionan que en la regulación de la *prueba electrónica* debe prevalecer el principio de libertad de prueba y que la evolución de la misma pasa por la no regulación. Esto es, consideran que la situación de admisibilidad actual es adecuada y no es necesario un cambio en el futuro.

  Otro cambio que los juristas estiman necesario llevar a cabo es una mejora de la comunicación entre los actores implicados en la admisibilidad de la *prueba electrónica*, entre aquellos responsables de la obtención, preservación y presentación de la misma en juicio y los jueces encargados de decidir sobre su admisibilidad. Los técnicos por el contrario, resaltan la importancia de aplicar cambios a nivel de protección de la privacidad de datos personales y la aplicación de políticas homogéneas en materia de seguridad.

VISIONES DE FUTURO:

- CONTRADICTORIAS SOBRE REGULACIÓN ESPECÍFICA.
- MEJORA DE LA COMUNICACIÓN.
- INCREMENTO EN LA PROTECCIÓN DE LA PRIVACIDAD DE DATOS PERSONALES.

PUNTOS CLAVE PARA LA MEJORA DE LA REGULACIÓN Y LA PRÁCTICA:

- LOS JUECES SON LOS ACTORES CENTRALES EN LA ADMISIBILIDAD DE LA *PRUEBA ELECTRÓNICA* Y LOS EXPERTOS DE LA POLICÍA OCUPAN UNA POSICIÓN PRINCIPAL EN LA OBTENCIÓN DE PRUEBAS. *ACTUEMOS SOBRE ESTAS DOS TIPOLOGÍAS DE ACTORES.*
- LA LEGISLACIÓN TIENE EL EFECTO DE INFLUIR POSITIVAMENTE EN LAS PERCEPCIONES DE SEGURIDAD QUE TIENEN LOS DIFERENTES AGENTES SOCIALES. *ADAPTEMOS LA LEGISLACIÓN EXISTENTE.*
- CONFIANZA EN LOS EXPERTOS RELACIONADOS CON LA OBTENCIÓN, ANÁLISIS Y CONSERVACIÓN DE LA *PRUEBA ELECTRÓNICA. SIGAMOS LOS PROCEDIMIENTOS TÉCNICOS DE LOS EXPERTOS.*
- FORMACIÓN, CONOCIMIENTO Y EXPERIENCIA SON LOS ELEMENTOS NECESARIOS E IMPRESCINDIBLES QUE TIENEN QUE REUNIR LOS EXPERTOS. *ACTUEMOS SOBRE LA FORMACIÓN.*
- LA MEJORA EN LA COMUNICACIÓN ENTRE LOS ACTORES RELACIONADOS CON LA *PRUEBA ELECTRÓNICA,* A NIVEL NACIONAL, EUROPEO E INTERNACIONAL, ES UN BIEN PRECIADO Y DESEADO UNÁNIMEMENTE. *MEJOREMOS EL ENTENDIMIENTO ENTRE JUECES Y TÉCNICOS.*

REFERENCIAS

- *Act on Electronic Services and Communication in the Public Sector.* Act n. 13 of 2003 in Finland Statutory Book. Finland.
- *Act on Electronic Signatures.* Act n. 14 of 2003. Finland.
- *Act on Provision of Information Society Services.* Act n. 458/2002 in Finland Statutory Book. Finland.
- BURT, R. S. (1982). *Toward a Structural Theory of Action: Network models of stratification, perception and action.* New York: Academic Press.
- BURT, R. S. (1992). *Structural Holes: The social Structure of Competition*. pp. 260-269. Cambridge, MA: Harvard University Press.
- BURT, R. S. (1997). "*The contingent value of social capital*", pp. 339-365. Administrative Science Quarterly n. 42.
- *Civil code.* DL 47 344 of 25 November 1966. Portugal.
- *Civil code.*1992.Updated at September 2001. Greece.
- *Civil evidence Act.*1995. United Kingdom.
- *Civil procedure code.* A.N. 44/1967 of 16-09-1968. Greece.
- *Civil procedure code*. DL 44-129 28-12-61 (Original code) DL 53/2004 updated version 18 March 2004. Portugal.
- *Code civil*. 8 mars 1803. 2004. Luxembourg.
- *Code civil.*1804. 2005. France.
- *Code de commerce.*15 septembre 1807. 2000. Luxembourg.
- *Code de commerce.* N. 2000/912 du 18 septembre 2000. 2005. France.
- *Code de justice administrative*. N. 2000-387 du 4 de mai. 2005. France.
- *Code de procédure pénale*. 2 mars 1959. 2005. France
- *Code d'instruction criminelle*. N. 447 du 22 septembre 1988. Modifié par Loi n.46/2006. Luxembourg.
- *Code du travail*. 2005. France.
- *Code of civil procedure*. 01/01/2002. Greece.
- *Code of judicial procedure.* N. 4 1734 in Statutory Book/chapter on evidence amended by 571/1948 and other sections by Act 690/1997. Finland.
- *Code of juridical procedure*. Promulgated in 1942, came into force on 1 January 1948. 1999. Sweden.
- *Codice civile*. Regio Decreto,n. 262 16/03/1942. Italy.
- *Codice di procedura civile*. Regio Decreto n. 1443, 28/10/1940. Italy.
- *Codice di procedura penale*. Decreto del Presidente della Repubblica n. 447, 22/09/1988. Italy.
- *Codice penale*. Regio Decreto, n. 1398, 19/10/1930. Italy.
- *Código civil* de 24 de julio de 1889. Actualizado 2000. Spain.
- *Código penal*. Ley n.10/1995 de 23 de noviembre 1995. 2005. Spain.
- *Codul civil*. N. 1655 4/12/1887 as amended by Decree 32/1954. Romania.
- *Codul commercial*. N. 1233 10/05/1887 as amended by Legea 99/1999. Romania.
- *Codul de procedura civila*. N. 11/1865. Amended 2005. Romania.
- Codul de procedura penala. 12/11/1968. Amended 2003. Romania.
- *Computer misuse act*. 1990. United Kingdom.
- *Constitution of Greece*. 11/06/1975 amended 2001. Greece.
- *Criminal code*. N° 39 of 1889 in Finland Statutory Book. Amendment Act 769 of 1990. Finland.
- *Criminal code.* Adopted in 1962, entered into force on 1 January 1965. 1999. Sweden.
- *Criminal evidence act*. N° 12 of 1992. Greece.
- *Criminal procedure act*. N° 689 of 1997 Finland Statutory Book. 1 October 1997. Finland.
- *Criminal procedure code*. 1/1/1951. Greece.
- *Decreto del Presidente della Repubblica* n. 445, 28/12/2000. *In materia di documentazione amministrativa*. Italy.
- *Decreto legislativo* n. 196, 31/12/2003, *Codice in materia di protezione dei dati personali*. Italy.
- *Decreto legislativo* n. 82, 07/03/2005. *Codice dell'Amministrazione digitale*. Italy.
- *Decreto legislativo* n. 373, 15/11/2000 Attuazione della *Direttiva N. 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato*. Italy.
- *Decreto legislativo* n. 286. 25/07/1998 *concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.* Italy.
- *Electronic commerce act*. N. 27 of 2000.Greece.
- *Electronic documents and signature*. Decree law 290-D/99 of 2 August 1999. Portugal.

- Freeman, L. Borgatti, S. y White, D. (1991). "Centrality in valued graphs: A measure of betweenness based on network flow" pp. 141-154 en Social Networks n. 13.
- *General Principles relating to international co-operation in the Council of Europe Convention on Cybercrime*. CETS 185 article 23.. Signature 23 november 2001. Ratified 12 may 2004. Entered into force 1 September 2004. Romania.
- *Grundgesetz* für die Bundesrepublik Deutschland vom 23.5.1949 (BGBl. I S. 1) zuletzt geändert durch Gesetz vom 28.8.2006 (BGBl. I S. 2034). Germany.
- Legea nr. 161 din 19 aprilie 2003 *privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei*. Romania.
- *Legea* nr. 365 din 7 iunie 2002 *privind comertul electronic*. Romania.
- *Legea* nr. 451 din 1 noiembrie 2004 *privind marca temporala*. Romania.
- *Legea* nr. 455 din 18 iulie 2001 *privind semnatura electronica*. Romania.
- *Legea* nr. 589 din 15 decembrie 2004 *privind regimul juridic al activitatii electronice notariale*. Romania.
- *Legge* n. 155 31/07/2005. *Misure urgenti contro il terrorismo*. Italy.
- *Ley 1/2000 de enjuiciamiento civil* de 7de enero de 2000. Spain.
- *Ley* 30/1992, de 26 de noviembre, de *Régimen jurídico de las administraciones públicas y del procedimiento administrativo común*. Spain.
- *Ley* 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico*. Spain.
- Ley 59/2003, de 19 de diciembre, de *firma electrónica*. Spain.
- *Ley de enjuiciamiento penal* de 14 de septiembre 1882. Modificada en 2003. Spain.
- *Ley de procedimiento laboral*. Real Decreto Legislativo n. 2/1995.2000. Spain.
- *Ley Orgánica* 6/1985, de 1 de julio, *del Poder judicial*.2005. Spain.
- *Loi* du 14 août 2000 *relative au commerce électronique*. 2004. Luxembourg.
- *Loi* du 24 mai 1989 *sur le contrat de travail*. 2005. Luxembourg.
- *Loi* du 28 novembre 2000 *relative à la criminalité informatique*. 28 novembre 2000. Belgium.
- *Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire*. 20 Octobre 2000. Belgium.
- *Loi modifiant le Code de la taxe sur la valeur ajoutée*. 5 décembre 2004. Belgium.
- *Loi relative au mandat d'arrêt européen*. 19 Décembre 2003. Belgium.
- *Loi relative aux droits des citoyens dans leurs relations avec les administrations*. Loi n°2000-321 du 12 avril 2000. France.
- *Loi transposant la directive 95/46/CE* du 24 octobre 1995 du Parlement européen et du Conseil *relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.* 1998-12-11. Belgium.
- Mérida (2004). *Redes cognitivas y sociales: análisis de las estructuras de los textos*. www.e-libro.net.
- *Nouveau code de procédure civile*. Septembre 1998. 2005. Luxembourg.
- *Nouveau code de procédure civile*.1995. 2005. France.
- *Criminal procedure code*. DL 400/82 of 23 September 1982. Portugal.
- *Personal data protection act*. 1st September 2001. Greece.
- *Police and criminal evidence act*.1984. United Kingdom.
- *Polizeigesetz Baden-Württemberg* in der Fassung vom 13.1.1992 (GBl. S. 1, ber. S. 596, 1993 S. 155) zuletzt geändert durch Gesetz vom 1.7.2004 (GBl. S. 469) m.W.v. 1.1.2005. Germany.
- *Regolamento per l'uso della posta elettronica certificata* DPR n.68 dell'11 febbraio 2005. Italy.
- *Retsplejeloven*. N. 90/1916 - 11 April 1916. Denmark.
- Rodríguez, J. A. (2006). *Análisis estructural y de redes*. Cuadernos metodológicos nº 16. Versión actualizada. Madrid. Centro de Investigaciones científicas (CIS). Pp.86.
- *Scope of procedural provisions in Convention on Cybercrime*. CETS 185 article 14 paragraph 2. Signature 23 November 2001. Ratified 12 may 2004. Entered into force 1 July 2004. Romania.
- *Strafprozessordnung* (StPO) vom 7.4.1987 (BGBl. I S. 1074, ber. S. 1319) zuletzt geändert durch Gesetz vom 12.8.2005 (BGBl. I S. 2360). Germany.
- *Strafprozessordnung* 1975 (StPO). BGBl 1975/631as amended by BGBl I 134/2002, 1st October 002 and 2005 (BGB I, 164/2005, BRÂG 2006). Austria.
- UCINET 6 Software. Analytic Technologies. PO Box 920089, Needham, MA 02492 USA.
- Wasserman, S. y Faust, K. (1994). *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press.
- *Zivilprozessordnung* in der Fassung der Bekanntmachung vom 5.12.2005 (BGBl. I S. 3202) geändert durch Gesetz vom 19.4.2006 (BGBl. I S. 866). Germany.

RESUMEN

LA ADMISIBILIDAD DE LAS *PRUEBAS ELECTRÓNICAS* EN LOS TRIBUNALES EUROPEOS ESTÁ REGULADA A TRAVÉS DE LAS DISPOSICIONES GENERALES DE LA PRUEBA TRADICIONAL EN EL CONJUNTO DE PAÍSES EUROPEOS, SIN QUE HASTA EL MOMENTO SE HAYA DESARROLLADO NINGUNA REGULACIÓN NACIONAL ESPECÍFICA EN EUROPA.

LAS PERCEPCIONES SUBJETIVAS MANIFESTADAS POR LOS ACTORES SOCIALES IMPLICADOS EN EL PROCESO DE ADMISIÓN DE LA *PRUEBA ELECTRÓNICA*, JUNTO AL VACÍO LEGISLATIVO EXISTENTE, EVIDENCIAN QUE ESTE TIPO DE PRUEBAS EN PARTICULAR, CONTRIBUYEN A GENERAR CIERTO GRADO DE INSEGURIDAD JURÍDICA Y PROFESIONAL. CONSECUENTEMENTE, EN SUS PERSPECTIVAS DE FUTURO, PERCIBEN LAS CARENCIAS Y RECLAMAN UNA FORMACIÓN, CUALIFICACIÓN Y REGULACIÓN ESPECÍFICAS, QUE CONFIERAN ESTÁNDARES Y GARANTÍAS SUFICIENTES PARA PROTEGER A LAS VICTIMAS DE DELITOS COMETIDOS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS.

PALABRAS CLAVE

PRUEBA ELECTRÓNICA, DERECHO PROCESAL, DERECHO COMPARADO, SOCIOLOGÍA DEL DERECHO, ADMISIBILIDAD, REDES JURÍDICAS, REDES COGNITIVAS Y EUROPA.

aec²

THE ADMISSIBILITY OF
ELECTRONIC EVIDENCE IN COURT
CYBEX INITIATIVE

CON LA COLABORACIÓN DE:

CONSEJO GENERAL
DEL PODER JUDICIAL

"la Caixa"

Grupo Intelligence Bureau: Pl. Cataluña, 20, 9º · 08002 Barcelona · Tel. 93 215 53 23 · Fax. 93 215 50 72
www.cybex.es