

I.- REUNIONES DEL GRUPO DE TRABAJO DE NUEVAS TECNOLOGÍAS, PREVENCIÓN Y SEGURO

- MEETINGS OF THE WORKING GROUP OF NEW TECHNOLOGIES

1.1-Reunión en Estambul el día 4 de mayo de 2012

Meeting of the Working Group on Istanbul, 4 Mai 2012

1.1 a.- Presentación del libro con las ponencias y comunicaciones del II Congreso de Nuevas Tecnologías, celebrado en Barcelona

1.1 b.- .English version of the presentation of the Book on New Technologies and Insurance (Papers of the II Conference on New Technologies)

1.2.- Liability and insurance related to damages caused by genetically modified organisms (GMOS)

1.3.a- Riesgos electrónicos

1.3.b- English versión of the paper “Electronic risks and insurance”

2- Next Meeting of the Working Group on New Technologies, Prevention and Insurance in London (Próxima reunión del Grupo de Trabajo en Londres) September, 13 2012.

3- III Congreso de Nuevas Tecnologías, Santiago de Chile, 12 y 13 de noviembre 2012 (III Conference on New Technologies, Santiago de Chile, November 12 -13)

II.- NOTAS DE ACTUALIDAD

III.- JURISPRUDENCIA

IV.- LEGISLACIÓN

I.-REUNIONES DEL GRUPO DE TRABAJO NUEVAS TECNOLOGÍAS, PREVENCIÓN Y SEGURO

1.1- Reunión en Estambul el 4 de mayo de 2012

La nueva reunión, después de la celebrada en mayo de 2011 en Asunción, trató diversos aspectos entre los que destacamos la presentación del libro con las ponencias del II Congreso de Nuevas Tecnologías, celebrado en noviembre de 2011 en Barcelona, España, por el Presidente del Grupo Joaquín Alarcón, seguida de una charla referente a “La responsabilidad y seguro referente a los daños ocasionados por los organismos genéticamente modificados”, por Teresa Rodríguez de las Heras, Vicepresidente del Grupo y una tercera comunicación, referida a “Los riesgos electrónicos y seguro”, a cargo del Secretario General del Grupo Félix Benito de Osma.

A continuación el resumen de las exposiciones:

1.1 a- Presentación del libro con las ponencias y comunicaciones del II Congreso de Nuevas Tecnologías, celebrado en Barcelona

Joaquín Alarcón Fidalgo, Presidente del Grupo de Trabajo

Las Nuevas Tecnologías (Internet, Biotecnología y Nanotecnología) tienen, como áreas multidisciplinares, diversas repercusiones en todos los ramos del seguro. Pero existe una considerable laguna de estudios doctrinales y también una importante falta de intercomunicación entre científicos y juristas.

La novedad de nuestros Congresos, que nuestro Grupo viene celebrando cada año, consiste en la convocatoria de científicos que plantean la situación actual de los riesgos derivados de cada una de las tres áreas, dando al mundo jurídico criterios adecuados para fijar la responsabilidad y al mundo asegurador para poder hacer el análisis adecuado del riesgo y estructurar debidamente las primas y condiciones de las pólizas.

El libro presenta diferentes aspectos de las tres áreas analizadas

INTERNET

1. Riesgos conectados con un sistema de información o con la red

Al evaluar el riesgo asociado a un sistema de información, tenemos que tener presente que las vulnerabilidades de los sistemas informáticos condicionan la eficacia de los mismos; consisten en un fallo o debilidad en el diseño, la implementación, el funcionamiento o la gestión de un sistema que puede ser violado. Además nos tenemos que enfrentar a ataques, acciones intencionadas llevadas a cabo por usuarios maliciosos y

las amenazas que son la posibilidad de violar una determinada política de seguridad.

Como sabemos, en el concepto de seguridad juega un papel importante el malware o código malicioso. Se trata de un tipo de software intrusivo y hostil, cuyo objetivo es infiltrarse o dañar un sistema de información sin la aprobación ni conocimiento de su propietario.

Se han detectado tres grandes categorías de malware:

el de propagación automática mediante infección vírica; .

el malware oculto, que intenta pasar desapercibido dentro del sistema infectado (rootkits, trayanos y puertas traseras o backdoors) y el malware lucrativo, que proporciona beneficio al atacante (Spyware, Ramsonware, Scareware, Bot, Adware Dialers).

Existen diversos métodos preventivos: prácticas del usuario (mantener actualizado el sistema operativo y aplicaciones, impedir descargas de software de fuentes no fiables, ignorar los correos de remitentes desconocidos), anillos de protección verificación de la autenticidad del código que se está ejecutando, mediante la firma digital etc.

La protección de la información es una necesidad pues en la red existen documentos, informaciones sensibles, dispositivos de almacenaje, comunicaciones etc que se ven amenazados en cuanto a su privacidad, autenticidad o integridad o que corren el riesgo del repudio.

Los mecanismos de protección como la clave simétrica o secreta y la clave asimétrica no siempre son seguros. Por otro lado, la complejidad del esquema criptográfico hace que las acciones no sean intuitivas para el usuario. Finalmente, falta agilidad a la hora de revocar los certificados.

Más complicado es conseguir la seguridad en las redes de tipo internet pues tienen vulnerabilidades congénitas (de diseño) y otras que son adquiridas (debidas a la implementación). Los ataques más frecuentes se dan por impersonación, por denegación de servicio, monitorización local, inundación/global, intrusiones debidas a fallos de configuración etc.

Los problemas en la seguridad de la red se dan, entre otros, porque el diseño de las aplicaciones se realiza por personas no expertas en seguridad, porque los sistemas son muy complejos con muchos elementos interaccionando, por la dificultad que aun tiene la informática forense y por vulnerabilidades congénitas difíciles de erradicar.

2. Los riesgos financieros

Nos encontramos con una serie de riesgos generados por actividades humanas, llevadas a cabo mediante el uso de soportes electrónicos y el eventual establecimiento de una obligación legal de adoptar medidas preventivas y proceder a su aseguramiento.

Entre estas nuevas responsabilidades podemos enumerar las que se originan en el juego electrónico, emisión de dinero electrónico y prestación de servicios electrónicos de pago. Entre los aspectos analizados, nos hemos centrado en el efecto deslocalizador, garantías exigibles a los operadores y forma de constituir las mismas (constitución de un seguro de caución), la reparación de los daños o el riesgo específico de salvaguarda de fondos.

3. Internet y su efecto en la suscripción del seguro

La oferta aseguradora se suele instrumentar a través de la página web de la aseguradora y mediante los agregadores o comparadores de precios. Pero estos agregadores tienen efectos negativos: incremento del coste de publicidad general por póliza, dilución del efecto de marca de la aseguradora e incluso ratios inferiores de retención del negocio.

Los motivos que llevan al cliente a elegir internet a la hora de contratar la póliza radican en la disponibilidad (24 horas, 365 días), rapidez, intimidad durante el proceso de análisis de la póliza y posibilidad de comparar productos y primas de muchas entidades de forma simultánea. Sin embargo el canal agencial tiene rasgos que siguen imperando como es la confianza en el mediador y solución de problemas una vez que se producen los siniestros.

4. El ciberperiodismo

La arquitectura actual de Internet es bidireccional y simétrica, centrada en el usuario; es un entorno de lectura- escritura interactivo en el que el usuario crea, amplia, varía o actualiza datos y contenidos.

Estas modificaciones en la arquitectura del medio digital crean consecuentemente nuevas rutinas de trabajo, dando lugar a nuevos perfiles periodísticos.

La interactividad propia de la Web 2.0 permite la participación activa del usuario del periodismo digital en la producción de noticias, sin control. El ciudadano normal que publica en actividades de periodismo ciudadano o cooperativo vulnera los mismos derechos que el periodista profesional, pero no tiene su cobertura legal ni empresarial.

Se plantean, a nivel particular, dos grandes problemas: el de si la infracción de derechos de autor y las lesiones a los derechos fundamentales están amparadas por la póliza familiar de responsabilidad civil y el de si puede ser amparado, al convertirse, en realidad, en un riesgo de la vida diaria. Por otro lado, la tipología del daño consiste normalmente en un perjuicio sin previo daño personal o material, lo que implicaría la revisión del condicionado.

El periodista profesional y, por supuesto su póliza de RC Profesional, tiene un nuevo escenario: el recibe la mayoría de las informaciones de usuarios privados en tiempo real que hace que la intensidad del riesgo se agrave por la falta de tiempo para contrastar la información.

5. Supuestos concretos

Como resumen, el Grupo de Trabajo está investigando diferentes casos concretos relacionados con la suplantación o robo de la identidad (impersonation), la seguridad y confidencialidad en el almacenamiento de datos(el caso Megaupload, el servicio "cloud computing con las cuestiones que afectan a la territorialidad, la propiedad intelectual, el destino y seguridad del contenido almacenado), la creación y explotación de programas que permiten el intercambio de archivos de audio etc. (P 2 P), la responsabilidad civil de los prestadores de servicios por comentarios alojados en sus páginas web, el uso de Internet para fines distintos a los autorizados en la vida laboral y en la diaria

INGENIERÍA GENÉTICA- BIOTECNOLOGÍA

Un organismo modificado genéticamente (OMGs) o transgénico es aquel cuyo material genético es manipulado en un laboratorio. En sí se trata de un conjunto de métodos que permiten cortar fragmentos de ADN de forma precisa, unirlos (recombinarlos, de ahí el nombre de tecnologías del ADN recombinante) e introducirlos en bacterias mediante vectores que son pequeños cromosomas o virus

Desde principios de los años 80 es también posible la modificación genética de animales. En cuanto a los humanos, la modificación genética es muy discutida, por lo que la prohibición de modificar un embrión humano para dar lugar a un individuo transgénico es generalizada en todo el mundo entre otros motivos por ser impredecible su resultado.

En las plantas es donde la modificación genética está más extendida.

Las modificaciones genéticas presentan problemas relacionados con la seguridad, los métodos de análisis de riesgo o los de tipo medioambiental.

La realidad es que la ciencia no puede afirmar que esta tecnología esté exenta de riesgos. Tenemos partidarios y opositores, ambos muy enfrentados. Los argumentos de ambos frentes están condicionados por la perspectiva de enfoque.

En Europa se aprobó en 1990 una Directiva sobre la liberación intencionada de OMGs, modificada en 2001 y 2002 e incorporada a los estados miembros. Un Reglamento CE del 2003 (nr. 1830/2003) estableció un marco para garantizar la trazabilidad y el etiquetado de OMGs.

El modelo regulatorio en Europa es, pues, profundamente precautorio, con un control previo riguroso que se basa en el sistema de autorización, etiquetado, trazabilidad y medidas de coexistencia).

Este marco regulatorio comunitario incluye un análisis detallado del riesgo, con una descripción molecular detallada de la modificación, análisis de la composición del producto, de la toxicidad y alergenicidad de la proteína introducida así como de los efectos sobre el medioambiente.

La nueva medicina se fundamenta en enfoques radicalmente distintos de la medicina tradicional y está centrada en la medicina regenerativa y medicina personalizada. La regenerativa presenta varios problemas (rechazo etc.). La medicina personalizada tiene también sus riesgos que se derivan del conocimiento exhaustivo del genoma del paciente, aplicando a partir de él un tratamiento individualizado para cada paciente en función de las características genéticas. El riesgo está en la interpretación y la comprensión de dicha información genética.

Existen múltiples técnicas de diagnóstico genético. De las seis mil enfermedades genéticas, unas dos mil se puedan ya diagnosticar mediante el análisis de los genes individuales. El proceso de análisis genético consta de unas 12 fases, en las cuales hay un trasiego de muestras entre laboratorio y clínica que genera diversos riesgos debidos a errores humanos, cruzamiento de muestras , errores de interpretación etc.

La libertad de las aseguradoras de utilizar la información genética predictiva en la evaluación del riesgo está siendo cada vez más puesta en duda, apoyándose en razones éticas y en los derechos fundamentales.

Los biobancos tienen destacada importancia en la industria biotecnológica, farmacogenética y farmacogenómica, pero dan lugar a una serie de interrogantes jurídicos que afectan a materias muy diversas como protección de datos, derechos fundamentales etc. Regulación de los biobancos sometida a normativa internacional de diverso tipo así como a diversos tipos de contratos, todo ello puede causar daños a las personas involucradas en la investigación o a terceros y dar lugar a responsabilidad contractual o extracontractual.

NANOTECNOLOGÍA

Un nanómetro es una unidad de longitud equivalente a la milmillonésima parte de un metro o una milésima parte de una micra; es la unidad natural para medir átomos y moléculas. Un nanoproducto está comprendido entre 0.1 y 100 nanómetros.

Los problemas ligados a la determinación de la nanorresponsabilidad y a la concreción de su seguro tienen diversas perspectivas, la mayoría de las cuales aún no están solucionadas. Entre otras:

- La definición y clasificación de los nanomateriales no goza de amplio consenso pues la ciencia está muy dividida a la hora de evaluar los nanomateriales y sus aplicaciones. A este respecto conviene tener en consideración la recomendación de la Comisión de la Unión Europea de octubre de 2011, respecto a la definición del nanomaterial: la definición del término debe estar basada solo en el tamaño de las partículas que constituyen el material, sin consideración del peligro o riesgo.
- La caracterización físico-química de las nanopartículas aún no está completa, dato que es esencial para poder relacionar las respuestas biológicas/ toxicológicas con sus propiedades.
- La toxicidad de una nanopartícula está relacionada estrechamente con su reactividad; si comparamos la nanopartícula con el material de mayor tamaño, vemos que la misma posee una relación superficie/volumen más elevada, lo cual incrementa el área de exposición exterior.
- Los efectos de superficie controlan muchas de las propiedades de los nanoobjetos a escala nanométrica. Un ejemplo: en una esfera su volumen es proporcional al cubo del radio, pero su superficie es proporcional al cuadrado del radio; conforme disminuimos el tamaño de la esfera la cantidad de volumen que contiene disminuye más rápidamente que la cantidad de superficie, lo que supone que al reducir la esfera a

dimensiones nanométricas muchas de las propiedades de los objetos vienen determinadas fundamentalmente por el estado de la superficie, con la consecuencia de que pequeñas modificaciones de este estado pueden dar lugar a grandes variaciones de determinadas propiedades físicas o químicas del nanoobjeto

- La enorme atención de que son objeto los nanomateriales se debe en parte a su potencial interacción con los sistemas vivos. Pero el estudio de la interacción entre objetos diseñados nanotecnológicamente y los sistemas biológicos tiene todavía muchas carencias, a veces por falta de conocimientos biológicos de los creadores de los nuevos materiales y por la disparidad de información existente, por ejemplo, sobre la nanotoxicología.

- La falta de normas estandarizadas en la nanotecnología. El Comité ISO/TC 229 es el encargado de generar las normas sobre nanotecnología que hagan posible comprender y controlar la materia y los procesos que acontecen en la escala nanométrica.

El sector asegurador se ve ante varios dilemas con respecto a la nanotecnología. Uno de ellos es que los nanoproductos, con sus cientos de aplicaciones, están incluidos en la cobertura de RC y otras al no estar expresamente excluidos. Otro es que se piensa que existe un riesgo potencial, extraordinario y aún solapado, que puede superar al que en su día conllevó el amianto.

Múltiples líneas de negocio están involucradas en el problema si tenemos presente que los productos nanotecnológicos y sus aplicaciones se extienden hoy prácticamente a todo tipo de industrias y bienes (en electrónica, en óptica, en biotecnología y en medicina, en cosméticos con nanopartículas, en tinta de copiadoras e impresoras, pañales de niños, en pinturas y recubrimientos, en textiles y en deporte, en pelotas, palos de golf, raquetas de tenis).

Esta omnipresencia de los nanoproductos puede llevar a que uno o varios productos ocasionen daños personales o materiales o bien considerables perjuicios económicos; la reclamación de los mismos afectará, sin dudas, a múltiples líneas de negocio y clases como responsabilidad civil general, productos, contaminación, umbrellas, retirada de productos, administradores y directivos, errores y omisiones, Rc patronal, accidentes de trabajo, automóviles y la mayoría de las líneas de daños.

La gerencia de riesgos en nanotecnología es otro de los problemas existentes: identificar, analizar y evaluar los nanorriesgos potenciales y sus posibles impactos en personas y medioambiente tienen absoluta prioridad, pero la cuestión es que la nanoindustria casi ha olvidado la investigación de los riesgos que presenta la nanotecnología. Un ejemplo: Mientras la UE está financiando diversos estudios en torno a la toxicidad potencial de los nanomateriales, tratando de desarrollar un marco regulatorio, la industria está vendiendo simultáneamente nanoproductos con riesgos potenciales que aún están siendo estudiados por los científicos.

1.1 b- English version of the presentation of the Book on New Technologies and Insurance (Papers of the II Conference on New Technologies)

The NT (Internet, Biotechnology and Nanotechnology) have as multidisciplinary areas important impact on all insurance branches. But there is considerable lack of doctrinal studies and also important lack of intercommunication between scientists and jurists.

The novelty of our NT Conferences, held by our Working Group each year, consists of the call of scientists that present the current risk situation of Internet, Biotechnology

and Nanotechnology, giving to the legal world appropriate criteria to establish responsibility and to the insurance to make proper risk analysis and fix the premiums and conditions of the policies.

The book looks at different topics.

INTERNET

1. Risks connected with the information systems and the networks

To assess the risk connected with an **information** system, we must bear in mind that the vulnerabilities in computer system determine the effectiveness thereof; they consist of defect or weakness in the design, implementation, operation or management. Moreover we have attacks, intentional actions by malicious users and the possibility to violate a given security policy. As you know in the concept of security the malware or malicious code plays an important role. It is a kind of intrusive and hostile software, whose objective is to infiltrate or damage a system of information without the consent or knowledge of the owner.

Three categories of malware have been identified: one of automatic propagation, through viral infection; the hidden malware and the lucrative malware.

There are several preventive methods: practices of the user (keep updated the operating system and applications, prevent downloads from software not reliable sources, ignore emails from unknown senders), protection rings, using the digital signature etc.

The information protection is a necessity because in the network there are documents, sensitive information, storage devices, communications ...that are threatening the privacy, authenticity or integrity. The protection mechanisms like the symmetric or asymmetric or public key are not always sure); on the other hand, the complexity of the cryptographic scheme makes that actions are not intuitive to the user. Finally, we have to fight with the lack of agility to revoke the certificates.

More complicated is to achieve security in the **networks**; they have congenital vulnerabilities (design) and other that are acquired (due to implementation). More frequent attacks occur by impersonation, denial of service, local monitoring, global flooding, intrusion due to configuration failures etc.

Security problems occur in the network, among others, because the design of applications is carried out by people who are not expert in security, the complexity of the systems with many elements interacting, the lack of computer forensics and the difficulty to eradicate congenital vulnerabilities.

2. Financial risks

We have a number of new risks generated by human innovation, activities carried out through the use of electronic media and the eventual establishment of the legal obligation to adopt preventive measures and usually to establish the assurance of these risks. The electronic game, electronic money and electronic payment are the main examples. There are any interesting issues related to the guarantees required (constitution of an insurance), to the repair of the damages or to the specific risks of safeguarding of funds.

3. Internet und its effect on the insurance underwriting

The insurance offer is usually made by the web page of the insurance company or through aggregators or comparators of price. But these have negative effects: increase of the marketing cost, brand dilution of the entity, antiselection and low retention rates.

The reasons which lead customer to choose internet lie in the availability (24 hours, 365 days), speed, privacy during the process and the ability to compare products and premiums of many entities simultaneously. But the agential channel continues to prevail as we trust in the insurance agent solving problems when a damage occurs.

4. Internet journalism

The current internet architecture is now bidirectional and symmetrical, focused on the user, it is an environment of reading, interactive writing in which the user creates, varies or updates data and contents.

These changes in architecture create new routines of work, giving rise to new journalistic profiles.

The web interactivity allows the active participation of the user without control. The normal citizen violates the same rights as a professional journalist, but has no the legal or firm coverage. We have here some insurance problems: the private liability policy does not cover copyright infringement or injury to fundamental rights, but they are now risks of the daily life. On the other hand, the professional journalist has a new scenario: he receives most of the news from private users, he is obliged to work in real time which makes greater the intensity of the risk by the lack of time to contrast the information.

5. Specific cases

Summarising: We are now analysing different concrete cases related to identity theft (impersonation), the security and confidentiality in data storage(case Megaupload, cloud computing, issues like territoriality, intellectual property, destine and security of the stored content), the creation and operation of programs that allow the exchange of audio files (P2P), civil liability of service providers for comments hosted on their websites, private use of internet by non authorized persons in working life etc.

BIOTECHNOLOGY/GENETIC ENGINEERING

A genetically modified organism (GMO) is the one whose genetic material is manipulated in a laboratory. Itself is a set of methods that allow to cut DNA fragments in a precise way, join them and introduce them in a specific bacteria through vectors that are small chromosomes or viruses. Since 1980 we have the genetic modification of animals. For humans the modification is very controversial, so the prohibition of modifying a human embryo to give rise to a transgenic individual is worldwide, among other reasons for being unpredictable results.

It is in plants where the genetic modification is more widespread.

The genetic modification problems are related to security, to risks analysis methods and to the environmental impact.

The reality is that science can not say that this technology is without risks.

We have supporters and people who oppose. The reasons are conditioned by the perspective.

In Europe a directive on the deliberate release of GMO was adopted in 1990 amended in 2001 and 2002 and in 2003 was established a framework to ensure the traceability and labelling. The European regulatory model is therefore deeply precautionary (prior control based on the system of authorization, labelling, traceability and coexistence measures).

This model also includes a detailed risk analysis related to the molecular description of the modification, to the product composition, to the toxicity and allergenicity and to the effects on the environment.

The new medicine is basically different from traditional medicine and is focused on personalized and regenerative medicine. The regenerative presents a number of problems (refusal). The personalized has also its risks arising from the knowledge of the genome of the patient, by applying a treatment individualized for each patient based on his genetic characteristics. But the risk is in the interpretation and understanding of such genetic information.

There are multiple techniques of genetic diagnosis. Six thousand genetic diseases, some two thousand can be already diagnosed through the analysis of individual genes. The process of genetic analysis consists of about 12 phases, in which there is an transfer of samples between laboratory and clinic that creates various risks due to human errors, cross-over of samples, errors of interpretation etc.

As you know, the possibility of insurers to use predictive genetic information on the risk assessment is increasingly being put in doubt, relying on ethical grounds and in the fundamental rights.

The biobanks have more and more importance, but give rise to a number of legal questions that affect fundamental subjects as data protection, rights etc. They are subjected to international regulations of various kinds as well as to various types of contracts, this can cause damage to persons involved in the investigation or to third parties and give rise to contractual or extra contractual liability.

NANOTECHNOLOGY

A nanometer is a unit of length equal to a billionth of a meter or a thousandth of a micron; it is the natural unit for measuring atoms and molecules. A nanoparticle is comprised between 0.1 and 100 nanometers.

The problems linked to the determination of the nano responsibility and the insurance cover have diverse perspectives, most of which are not resolved. Among others:

- The definition and classification of the nanomaterials do not enjoy broad consensus, the science is divided in evaluating the nanomaterials and their applications. It is important in respect to this the EU Commission Recommendation of October 2011, concerning the definition of nanomaterial: the definition of the term must be based only on the size of the constituent particles of a material, regardless of the danger or risk.

- The physicochemical characterization of nanoparticles is not completed, but this is essential to be able to relate the biological/toxicological responses with their properties.

- The toxicity of a nanoparticle is closely related to its reactivity. If we compare the nanoparticle with the material of greater size, we can see that it has a higher surface/volume relation, which increases the outside exposition area.
- The surface effects control many of the properties of a nanoproduct. If we cut an apple, f. e., the amount of volume that it contains decreases faster than the surface amount. What does it mean? It means that by reducing the field to nanodimensions many of the properties of the material are determined basically by the state or condition of the surface; the result is that small changes in this state may give rise to large modifications of certain physical or chemical properties of the nanobject.
- The great attention to the nanomaterials, everyone looks at them, is due in part to their potential interaction with living systems, but the study of these interactions present still many deficiencies, due sometimes to the lack of biological knowledge of the inventors and also to the disparity of information on nanotoxicology.
- The lack of standard patterns, of norms in nanotechnology. The ISO Committee TC 229 is responsible for generating standards on nanotechnology that will make possible to understand and control the materials and processes in the nano scala.

The insurance industry is faced with several dilemmas: one of these is that the nanoproducts and applications are included in the coverage because they are not explicit excluded. On the other side the insurance thinks that there is a risk potential similar to the asbestos. Multiple lines of insurance are involved when we think that the nanoproducts and its applications extend today practically in all kinds of industries and property (in electronics, optics, biotechnology and medicine, cosmetics, ink copiers and printers, in paints and coatings, in textiles, in sport (balls, racquets). This omnipresence of the nanoproducts can lead to one or several products to cause personal injury or property damages affecting the general liability, products, pollution, umbrellas, recall, D&O, errors and Omissions policies etc.

The risk management related to nanotechnology is other of the existent open problems: identify, analyse and assess the potential nanorisks and their impacts on people and environment have absolute priority, but the question is that the nanoindustry has near forgotten the necessary research on the risk posed by nanotechnology. An example: while the EU is funding several studies on the potential toxicity of nanomaterials, trying to develop a regulatory framework, the industry is selling simultaneously nanoproducts with potential risks that are still being studied by scientists.

1.2. Liability and insurance related to damages caused by genetically modified organisms (GMOS)

Prof. Dr. Teresa Rodríguez de las Heras, Vice- President of the Working Group on New Technologies

A). General Overview

Modern biotechnology, in particular, applied to agricultural practices and food industry ("green biotechnology"), has infused our modern risk society with its connatural uncertainty that has triggered a much widely reluctant social perception against and diverging market responses. Indeed, an all-embracing approach to biotechnology results from a delicate balance among several converging forces: scientific-technical, social, economic and legal factors. From their interaction, a particular conception and regulation on GMOs derives.

Firstly, the innate scientific uncertainty underlying modern scientific and technical progress tarnishes social perception on biotechnological applications, in particular, in relation to agriculture, farming methods and food industry. Unlike a favorable attitude towards some biotechnological applications such as bioremediation or biodiversity-preserving technologies, skepticism and generalized concern persist in relation to bio-agro developments. Such a reluctant view is indistinctively based on ethical concerns, effects of alimentary crisis and an increasing ecology sensibility.

Secondly, scientific uncertainty permeating technical progress has also highly determined the regulatory approach to GMOs. Two legal solutions do clearly reveals how legislators manage uncertainty in the lawmaking process: the precautionary principle (caution in advance) and the “state of scientific and technical knowledge” defense (development risk defense).

Thirdly, social perception and market response to GMOs are normally closely linked. Whereas a receptive social stance is usually followed by an increasing development of the GM-market, some legal obligations, at the same time, on the business’ side improve consumers’ perception on GM-products: labeling, traceability obligations, and coexistence measures. Nevertheless, the coexistence model aimed at ensuring consumers’ and producers’ free choice among Genetically Modified, conventional and organic crops and products is debated in Europe since it is considered that it represents a indirect permission to transgenic pollution. In fact, in parallel to the increasing expansion of “GM-free zones” in Europe, companies in biotechnology industry are moving out from European countries to other regions. Ethical concerns, unexpected damages on human health and ecologist movements are behind of the European reluctant position but the fear of the so-called “genetic imperialism” likely to be enabled by a growing number of patent concessions has intensified social distrust against biotechnological companies.

Finally, all abovementioned factors do converge on a regulatory model on GMOs based on the following elements: precautionary principle, rigorous ex-ante measures, close supervision and risk prevention.

The aim of this talk is to identify possible liability issues related to GM-crops and GM-derived products. The paper is mainly focused on environmental damages caused by GMOs but other possible liability cases are briefly referred to as well.

The study of environmental liability rules currently in force in the European Union and in Spain reveals that, even if it can be clearly concluded that environmental damages caused by GM-crops do fall within the legal scope, the scheme of exclusions, limitations and waivers significantly limits the effectiveness of the legal model to prevent and remedy environmental damages caused by GMOs. Accordingly, it does strongly depend on insurance policies, financial guarantees and compensation funds. Not surprisingly, such a conclusion should condition the development of insurance products and markets. And it encourages constructing liability regimes on an integral and comprehensive basis with the aim of ensuring deterrence of harming activities and full compensation of potential damages.

A.1.- Liability cases

Should the study be focused on damages likely to be caused by GM-crops and derived products, at least four potential liability cases can be reasonably foreseen:

1.- Environmental damages. GM-crops might cause damage to aquatic environment, contaminate land, adversely affect biodiversity or cause air pollution. These damages are likely to fall within the concept of environmental damage under EU environmental liability rules.

2.- Purely economic losses. In a model of coexisting farming techniques, adventitious presence of GM-material in neighbouring conventional or organic crops might be the main cause of economic losses on other producers and farmers arising from the eventual loss of organic label for exceeding tolerance threshold of organic purity, a resulting decrease of sales, the need of additional expenses to prevent or remedy contamination, re-labelling, or breach of existing contracts requiring organic purity.

3.- Harm to persons. Considering that GM-derived products are expected to introduce in food market, harm to human health due to toxicity or allergenic reactions is possible. Accordingly, application of defective product liability rules should be carefully considered.

4.- Patent violation. In the context of adventitious presence of GM-products in conventional or organic crops, an anomalous and surprising situation is likely to arise. In absence of previous licenses or agreements between neighbouring farmers, GMOs presence in other crops could be account for violation of patent rights hold by GM-crop farmer.

A.2.- Damages caused by GMOs: special features

Damages caused by biotechnology applications, in particular, as far as agriculture and food industry are concerned, reveal some special features that hinder a straight application of traditional liability rules:

Diffuse damages

That appear on a gradual basis

Having a cumulative effect

Potentially massive

Whose harming impact may manifest and persist in long-term

Unexpected damages whose monitoring, prevention and remediation do strongly depend on state of art

Complex chain of factors concurring in resulting damages

Not surprisingly, the assessment of causation and the identification of tortfeasors are frequently a complex task that involves a significant effort to provide scientific evidences, sometimes uncertain, to verify elements proving liability.

A.3.- Differences between Civil liability and Environmental liability

Last decades, EU has struggled for defining an adequate legal framework to enforce “polluter pays principle” in line with sustainability goals under a Community environmental policy. After several assessment reports, studies, environmental action programs and the White Paper on Environmental Liability, Directive 2004/35/EC[1] is enacted. Law 26/2007, 23 October, on Environmental Liability introduces Community rules into the Spanish legal system (Spanish Environmental Liability Act) implementing Article 45 of Spanish Constitution 1978 as well that enshrined the right to an adequate environmental and the duty to restore the damaged natural resources.

European Environmental Liability model is based on four distinguishing features:

EU Directive does not prejudge a legal model to be implanted for preventing and remedying environmental damages. It aims at providing a common framework for enabling Member States to recover decontaminating cost to remedy damaged environment. With such an aim, a set of supervisory powers is provided for. Therefore, it is essentially a public-law model entailing an administrative approach considering that civil liability approach better fits "traditional damages" – damage to property, personal injury and economic losses -. Environmental Liability Directive does not apply to cases of personal injury, to damage to private property or to any economic loss and does not affect any right regarding these types of damages.

It is a full-restoration model aiming to ensure that prevention and remedial measures are properly taken to restore damage natural resources and services to baseline condition.

It is essentially a strict liability model even if, in more depth, it works as a modular system with different scopes depending on kind of measures to be adopted combining strict liability rules and fault-based criteria.

It is inspired by a strong preventive goal. Indeed, not only actual damages but also mere "imminent threat of such damages occurring" triggers the duty to adopt preventive measures.

A.4.- Legal framework for Environmental liability: core elements, legal concept of environmental damage and exclusions

The legal concept of environmental damage is provided for by EU Directive as follows:

1. "environmental damage" means a measurable adverse change in a natural resource or measurable impairment of a natural resource service which may occur directly or indirectly, in particular,

(a) damage to protected species and natural habitats, which is any damage that has significant adverse effects on reaching or maintaining the favourable conservation status of such habitats or species. The significance of such effects is to be assessed with reference to the baseline condition, taking account of the criteria set out in Annex I;

Damage to protected species and natural habitats does not include previously identified adverse effects which result from an act by an operator which was expressly authorised by the relevant authorities in accordance with provisions implementing Article 6(3) and (4) or Article 16 of Directive 92/43/EEC or Article 9 of Directive 79/409/EEC or, in the case of habitats and species not covered by Community law, in accordance with equivalent provisions of national law on nature conservation.

(b) water damage, which is any damage that significantly adversely affects the ecological, chemical and/or quantitative status and/or ecological potential, as defined in Directive 2000/60/EC, of the waters concerned, with the exception of adverse effects where Article 4(7) of that Directive applies;

(c) land damage, which is any land contamination that creates a significant risk of human health being adversely affected as a result of the direct or indirect introduction, in, on or under land, of substances, preparations, organisms or micro-organisms.

Starting from the above-transcribed concept of environmental damage, the European environmental liability system is based on four pillars:

1.- Environmental damage or imminent threat of such damage occurring

It entails firstly a “measurable adverse change in a natural resource” and secondly one or several natural resources or services falling within the legal notion of environmental as defined for protection purposes: protected species and natural habitats, water and land to the extent that land contamination creates a significant risk of human health. Thus, the legal approach to the elusive notion of environment is based on segmentation strategy resulting in a multi-factor definition – mixing anthropocentric and ecocentric criteria - but not on a comprehensive one.

2.- Occupational activities

According to EU Directive, a two-layer environmental scheme is provided for. The first liability scheme is a strict liability scheme. Therefore, no fault is required. The strict liability scheme applies to the presumed dangerous or potentially dangerous occupational activities listed in Annex III that expressly includes activities related to genetically modified organisms and micro-organisms. The second liability scheme applies to all occupational activities other than those listed in Annex III and requires fault or negligence. Besides, in the case of the EU Directive, unlike the wider Spanish version, the operator will only be held liable if there is damage or imminent threat of damage to species or natural habitats protected by Community legislation.

The above-explained model responds to a precautionary strategy aiming to discourage potentially risky activities, improve prevention mechanisms and internalize environmental costs in business activities.

3.- Risk or fault

Nevertheless, the scope of obligations widens if the operator undertaking any occupational activity other than those listed in Annex III acts at fault or negligently. Thus, should no fault or negligence occurs, the operator will not be held to adopt remedial measures, but only prevention measures.

4.- Causation

Assessing causation entails a high complexity when involving environmental damages and, in particular, harms of a diffused character. Even if an intention to presume causation in certain situations, concretely those regarding activities listed in Annex III, does apparently be inferred from legal provisions, it cannot be sustained that environmental liability model intends to remove causation from liability rules. Causal link is still a prerequisite for declaring liability.

A set of limitations and exclusions narrows the scope of EU environmental liability rules in relation to damages caused by GM-crops and GM-derived products:

a). Diffuse damages. According to Article 4, Directive shall only apply to environmental damage or to an imminent threat of such damage caused by pollution of a diffuse character, where it is possible to establish a causal link between the damage and the activities of individual operators

b). International Treaties. Maritime claims or nuclear risks.

c). Time limits. Articles 17 and 19 Directive: This Directive shall not apply to:
- damage caused by an emission, event or incident that took place before the date referred to in Article 19(1),

- damage caused by an emission, event or incident which takes place subsequent to the date referred to in Article 19(1) when it derives from a specific activity that took place and finished before the said date,
- damage, if more than 30 years have passed since the emission, event or incident, resulting in the damage, occurred.

d). Defenses. In Article 8, two defenses, especially relevant for GMO-activities, are provided for. Member States upon the transposition of the Directive into domestic legislation are entitled to establish or not those defenses.

Accordingly, an operator shall not be required to bear the cost of preventive or remedial actions taken pursuant to this Directive when he can prove that the environmental damage or imminent threat of such damage:

- (a) was caused by a third party and occurred despite the fact that appropriate safety measures were in place; or
- (b) resulted from compliance with a compulsory order or instruction emanating from a public authority other than an order or instruction consequent upon an emission or incident caused by the operator's own activities.

In such cases Member States shall take the appropriate measures to enable the operator to recover the costs incurred.

The Member States may allow the operator not to bear the cost of remedial actions taken pursuant to this Directive where he demonstrates that he was not at fault or negligent and that the environmental damage was caused by:

- (a) an emission or event expressly authorized by, and fully in accordance with the conditions of, an authorization conferred by or given under applicable national laws and regulations which implement those legislative measures adopted by the Community specified in Annex III, as applied at the date of the emission or event; (permit defense)
- (b) an emission or activity or any manner of using a product in the course of an activity which the operator demonstrates was not considered likely to cause environmental damage according to the state of scientific and technical knowledge at the time when the emission was released or the activity took place. (development risk defense).

A.5.- Environmental insurance: binding character, characteristics, insurance practice (coverage, time limits, exclusions)

Only 8 States, including Spain, has opted for a compulsory scheme for financial security with a clear preference for insurance products subject to time limits, amount limits (20 millions Euros), de minimis threshold and a step-by-step implementation.

The system is supplemented by the establishment of compensation funds.

B). Sector-based approach: GMOs in particular GM-crops and products

B.1- Concept

According to Article 2.2 Directive 2001/18/EC "Genetically Modified Organism (GMO)" means an organism, with the exception of human beings, in which the genetic material has been altered in a way that does not occur naturally by mating and/or natural recombination. Within the terms of this definition:

- (a) genetic modification occurs at least through the use of the techniques listed in Annex I A, part 1[2];

(b) the techniques listed in Annex I A, part 2, are not considered to result in genetic modification^[3].

B.2.- International situation: pros and cons

As briefly stated above under A) General Overview.

B.3.- Regulatory models

EU White Paper on Environmental Liability, 2000.

B.4.- Damages likely to be caused by GMOs
See A.1. above.

B.5.- Causal link. The problem of diffuse damages

Not all forms of environmental damage can be remedied by means of the liability mechanism. For the latter to be effective, there need to be one or more identifiable polluters, the damage should be concrete and quantifiable, and a causal link should be established between the damage and the identified polluter(s). Liability is therefore not a suitable instrument for dealing with pollution of a widespread, diffuse character, where it is impossible to link the negative environmental effects with acts or failure to act of certain individual actors

B.6.- Cases where liability is waived

An operator should not be required to bear the costs of preventive or remedial actions taken pursuant to the Environmental Liability Directive in situations where the damage in question or imminent threat thereof is the result of certain events beyond the operator's control. Member States may allow that operators who are not at fault or negligent shall not bear the cost of remedial measures, in situations where the damage in question is the result of emissions or events explicitly authorised (permit defence) or where the potential for damage could not have been known when the event or emission took place (development risk defence).

1.3. a Riesgos electrónicos y seguro

Prof. Dr. Félix Benito de Osma

1. Evolución de las Tecnologías de la Información y Comunicación (TIC)

El equipamiento TIC y el acceso a conexión de banda ancha en el año 2011 evoluciona notablemente en los hogares españoles y europeos. Las TIC representan, en cuanto a facturación, el 10% del PIB español, según el informe anual La Sociedad en Red 2011 elaborado por el Observatorio Nacional de la Telecomunicaciones y de la Sociedad de la Información (ONTSI)

La implantación de las TIC es toda una realidad en todos los sectores económicos, incluido el asegurador (con multiplicidad de canales, aceptación de coberturas por las entidades aseguradoras a través de su página web u otras creadas "ad hoc", así como el establecimiento de canales de comunicación con la clientela, multitarificador unida a la página web del intermediario de seguros) y en la autoridad supervisora (portal del asegurado que ofrece información a los ciudadanos sobre sus derechos, los mecanismos de defensa y el servicio de reclamaciones vía telemática).

Internet no es sólo marketing ni un canal de venta de un producto sino un proceso de hacer negocios con la prestación de un servicio. Se trata de una redefinición del proceso encaminado no ya a la propia venta sino, más allá, a prestar un servicio concreto y completo ajustado al peticionario.

2. Riesgos electrónicos y seguro

Internet refleja la sociedad que vivimos, no exenta de riesgos. Por tanto, como la vida la misma, no hay una seguridad plena y global. Los riesgos no son alterados por el cambio de medio o el comportamiento de las personas que supone esta revolución tecnológica. Son los mismos conforme al principio de neutralidad tecnológica, pero hay que evaluar la medida de riesgo y la probabilidad de ocurrencia. Para ello, la gestión de riesgos ha de ser administrada como un negocio dentro de la empresa, como una parte integral de la estrategia empresarial, profesional e institucional que contribuye a la satisfacción de los objetivos marcados por aquéllas. Estamos, pues, en un proceso de transformación en el que todavía es pronto su evaluación.

Los riesgos asegurables relacionados con el uso de las TIC o del entorno electrónico se clasifican en daños en las cosas o en el patrimonio, responsabilidad civil, asistencia y otros referidos a la salud, accidentes y medioambiental. Existen nuevos seguros con coberturas específicas: seguros de equipos informáticos, seguros de consultoría y asistencia informática, seguros de pérdidas de datos, seguro de protección de datos, seguros de redes sociales, además de las pólizas que quedan afectadas. Las pólizas tradicionales de daños no protegen estos nuevos riesgos de importantes consecuencias negativas a las compañías, por la pérdida o sustracción de datos informáticos confidenciales y de reputación empresarial.

La cloud computing constituye un modelo de prestación de servicios tecnológicos, a través de la red, como es el correo electrónico, almacenamiento de documentos.... Este mecanismo refleja naturalmente riesgos referidos a la seguridad, a la privacidad y a confidencialidad de los datos. Tanto el prestador como su peticionario están expuestos a responsabilidades en cuanto al acceso, conocimiento y tratamiento de la información.

3. Responsabilidades electrónicas: administradores y profesiones jurídicas.

Los administradores de las sociedades de capital tienen el deber de mantener lo insertado en la página web durante el término exigido por la ley, y responderán solidariamente entre sí y con la sociedad frente a los socios, acreedores, trabajadores y terceros de los perjuicios causados por la interrupción temporal de acceso a esa página, salvo que la interrupción se deba a caso fortuito o de fuerza mayor. Para acreditar el mantenimiento de lo insertado durante el término exigido por la ley será suficiente la declaración de los administradores, que podrá ser desvirtuada por cualquier interesado mediante cualquier prueba admisible en Derecho.

Las profesiones jurídicas en general (secretario judicial, procurador, abogado, notarios) pueden incurrir en responsabilidad derivada de las comunicaciones y notificaciones electrónicas(por ejemplo casos de suplantación de identidad). Los notarios quedan afectados en varios supuestos como son la constitución telemática de las sociedades de capital y en el acceso telemático al Registro de condiciones generales de la contratación.

4. La actividad aseguradora y el seguro en un entorno electrónico

El sector asegurador se encuentra en pleno proceso de reestructuración electrónica como consecuencia del entorno competitivo; sus esfuerzos van encaminados a mejorar la competitividad y crear nuevos productos eficaces mediante la utilización de las herramientas electrónicas. De ahí surge la necesidad de la implantación generalizada del entorno electrónico con el acceso a los nuevos canales de comunicación y de distribución.

La revolución tecnológica debe pasar por la creación de nuevos seguros y la adaptación de las pólizas vigentes a los nuevos riesgos electrónicos generados por el desarrollo económico y social. Debe ser una prioridad para el sector asegurador, pues el cambio estratégico, comercial y cultural pasa ineludiblemente por el contrato de seguro. El seguro sirve como elemento de auxilio y complemento a este proceso de transformación en las comunicaciones, operaciones y responsabilidades electrónicas que está demandando la sociedad civil y económica.

La implantación electrónica íntegra vendrá determinada por el análisis y gestión de los riesgos, fundamentalmente dentro del gobierno corporativo de las propias empresas, con la participación inexcusable de las aseguradoras y de los intermediarios o asesores de seguros. Estamos, pues, ante un campo de actuación y de negocio abierto generado precisamente por la revolución técnica y tecnológica a la que estamos inmersos en el que el contrato de seguro ha de jugar un papel importante. El sector asegurador en su sentido más amplio ha de ser la figura coadyuvante en este proceso de cambio y de desarrollo y el seguro el complemento a toda estrategia o plan integral de gestión de riesgos de la actividad necesariamente interdependiente.

1.3. b- English versión of “Electronic risks and insurance”

Prof. Dr. Félix Benito de Osma

1. ICT developments

ICT equipment and access to broadband connection in 2011 evolved dramatically over the Spanish and European homes. ICT is, in terms of turnover, 10% of Spanish GDP, according to the annual The Network Society 2011 prepared by the National Observatory of Telecommunications and Information Society (ONTSI).

The implementation of ICT is a reality in all economic sectors, including insurance (with multiple channels, acceptance of coverage by insurance companies through its website or other created "ad hoc" and the establishment of communication channels with customers, multitarificador linked to the website of the insurance intermediary) and the supervisory authority (secured portal that provides information to citizens about their rights, defenses and claims service computer).

Internet marketing is not just a sales channel or a product but a process of doing business with the provision of a service. This is a redefinition of the process of not only the sale itself but beyond, to provide a specific service and complete set of the petitioner.

2. New electronic risks

Internet reflects the society we live in, not without risks. Therefore, the same as life, there is a full and comprehensive security. The risks are not altered by the change of environment or behavior of people involved in this technological revolution. They are the same according to the principle of technological neutrality, but we must assess the extent of risk and likelihood of occurrence. To do this, risk management must be managed as a business within the company, as an integral part of business strategy,

professional and institutional contributes to meeting the objectives set by them. We are therefore in a process of transformation in which it is still early evaluation.

Insurable risks related to the use of ICT or the electronic environment are classified as damage to things or in equity, liability, assistance and referrals to other health and environmental accidents. There are new insurance with specific coverage: insurance computers, insurance consulting and computer support, data loss insurance, insurance, data protection, safe social networking, as well as policies that are affected. Traditional policies do not protect from damage the new risks of significant adverse effects on companies, the loss or theft of confidential computer data and business reputation.

Cloud computing is a model of technological services, through the network, such as email, document storage This mechanism reflects risks relating to security, privacy and confidentiality of data. Both the lender and your petitioner are exposed to liability in terms of access, knowledge and information processing.

3. New electronic liabilities. Managers of corporations and legal professions.

Specifically, the managers of corporations have a duty to keep the insert in the website for the term required by law, and jointly liable with each other and society from shareholders, creditors, employees and third parties for damages caused by the temporary disruption of access to that page, unless the interruption is due to unforeseeable circumstances or force majeure. To prove the maintenance of the insert during the term required by law will be sufficient declaration of the directors, who may be invalidated by any party by any evidence admissible in law.

The liabilities of the legal professions (court clerk, prosecutor, lawyer and notary) in communications and electronic notification and identity theft and, especially, responsibility and liability insurance required of the notary in the constitution telematics capital companies and on the other hand, in the telematic access to the Registry of general conditions of contract.

4. The insurance business in an electronic environment

The insurance industry is in the process structure as a result of the competitive environment and its efforts are aimed at improving the competitiveness from the standpoint of technical and operational, with the creation and launch of new products swiftly and efficiently. Hence the need of their widespread deployment of access to new channels of communication and distribution.

Insurance can not be a stranger to this technological revolution. The implementation of new insurance and adaptation of existing policies to new electronic risks generated by the economic and social development should be a priority for the insurance industry, for strategic change, trade and cultural unavoidably by the insurance contract. Must serve and serving as a relief and a complement to this process of transformation in communications, electronic operations and responsibilities is demanding civil and economic society.

The advancement or preparation is determined by the analysis and risk management by the companies within its corporate governance with the participation inexcusable insurers and intermediaries or insurance advisors. We are therefore faced with a level playing field and open business generated precisely by the technical and technological revolution to which we are engaged in the insurance contract must play an important role. The insurance sector in its broadest sense should be the adjuvant contained in this process of change and development and safe addition to any strategy or comprehensive plan of risk management activity necessarily interdependent

2. Next Meeting of the Working Group on New Technologies, Prevention and Insurance in London (Próxima reunión del Grupo de Trabajo en Londres)

Date: 13 September, 2012

Description:

Legal issues arising from the provision of services enabling business transactions and social relationships in the digital space: electronic intermediation, cloud computing, network securities. Environmental liability and insurance: challenges and realities. Genetically Modified Organisms (GMOs): Risks, liability cases and insurance.

PROGRAM

I.- Opening remarks and welcoming words

II.- Presentation of the Book on New Technologies and Insurance (Proceedings of the *II Conference on New Technologies*)

III.- Future activities: *III Conference on New Technologies and Insurance*, November 2012

IV. - Topic to discuss:

IV.1.- Internet and Insurance: spotting new risks and emerging liabilities

1. Network security: suitable tools, frequent attacks and protecting mechanisms
2. Cloud computing: legal concerns related to security issues and data confidentiality. Data protection.
3. The development and exploitation of P2P software enabling file sharing: problems, actions to be undertaken and potential damages
4. ISP liability on grounds of third parties' comments published or hosted on their websites. The issue of the neutral position.
5. New electronic liabilities: electronic gambling, electronic money and payment services provision

IV.2.- Liability and Insurance related to damages caused by Genetically Modified Organisms (GMOs): Environmental damages and purely economic damages

A) General Overview

1. Damages caused by GMOs: special features
2. Differences between Civil liability and Environmental liability
3. Legal framework for Environmental liability: core elements, legal concept of environmental damage and exclusions
4. Environmental insurance: binding character, characteristics, insurance practice (coverage, time limits, exclusions)

B) Sector-based approach: a Case Study – Genetically Modified Crops

1. International situation: pros and cons
2. Regulatory models

3. III Congreso de Nuevas Tecnologías, Santiago de Chile, 12 y 13 de noviembre 2012 (III Conference on New Technologies, Santiago de Chile, November 12 -13)

Sede: Universidad de Los Andes, Santiago de Chile

PROGRAMA

Día 12 de Noviembre

8:30h APERTURA

Dr. D. Orlando Poblete. Rector de la Universidad de los Andes
Dr. D. José Manuel Camposano. Presidente de la Asociación de Aseguradores de Chile
Presentador: Dr. D. Andrés Amunátegui Echevarría, Centro de Derecho de Seguros. Universidad de los Andes.

9:00h Primera sesión: INTERNET

Moderador: Dr. D. Ricardo Peralta Larraín. Universidad de Chile.

9:00h: “Seguridad y confidencialidad en el uso, tráfico y almacenamiento de datos (suplantación de identidad, cloud computing, protección de datos)”
Dr. D. Joaquín Alarcón Fidalgo. Abogado. Secretario General de SEAIDA.

09:30h: “Intermediación electrónica y generación de confianza en la Red: escenarios de riesgos y responsabilidad”
Dra. D^a. Teresa Rodríguez de las Heras, Universidad Carlos III, Madrid

10:00h: “El tráfico de la información en la web 2.0: nuevos escenarios de riesgo y de responsabilidad”
Dr. D. Félix Benito Osma, Universidad Carlos III, Madrid

10:30h: CAFÉ

11:00h: “El ciberacoso laboral y privado en la red: nuevas responsabilidades”
Dra. D^a. María José Morillas, Universidad Carlos III, Madrid

11:30h: “Internet y su efecto en la suscripción del seguro”
Dr. D. Eduardo Sánchez Delgado. Director del Área actuarial de MAPFRE.

12:00h: “Los registros electrónicos del contrato de seguro (Vida y Seguros Obligatorios)”
Dr. D. Rafael Illescas, Universidad Carlos III, Madrid

Segunda sesión: BIOTECNOLOGÍA E INGENIERÍA GENÉTICA

Moderadora: Dra. D^a. Mercedes Sanz, España

12:30h: “La respuesta inmune y su implicancia en la salud humana”
Dr. D. Alexis Kalergis, Universidad Católica de Chile

13:00h: ALMUERZO

14:30h: “Terapia celular”

Dr. D. Maroun Khoury, Universidad de Los Andes, Chile.

15:00h: “Acceso a la información genética, sus riesgos y la posible discriminación”

Dr. D. Alonso Núñez del Prado. Abogado. Presidente de AIDA Perú.

15:30h: “El interés asegurable en los riesgos de la medicina genética. Las partes interesadas en la contratación y la indemnización aseguradora”

Dra. D^a. Marcia Cicarelli Barbosa de Oliveira, Abogada de JBO, Brasil.

16:00h: CAFÉ

16:30h: “Las modificaciones genéticas. Naturaleza y frecuencia de la enfermedad genética”

Dra. D^a. Silvia Nora Carbognani. Universidad Nacional del Rosario. Argentina.

17:00h: “Estado actual de la medicina genómica: balance y perspectivas”

Dr. D. Luis Fidel Tejeda Macedo. Universidad Nacional de San Agustín, Arequipa-Perú.

17:30h: “La contaminación medioambiental por organismos genéticamente modificados”

Dr. D. Joaquín Alarcón Fidalgo, España y D^a. Patricia Jaramillo Salgado, Gerente de Regulación de Protección, Colombia.

18:00h: “La responsabilidad civil derivada de las modificaciones genéticas, con especial referencia al “doping” genético en la actividad deportiva”

Dr. D. Eduardo Mangialardi, Universidad Nacional de Rosario, Argentina

18:30h: “Las coberturas existentes. Necesidades. El reaseguro”

Dr. D. Sergio Barroso de Melo, Brasil, Presidente del CILA

19:00h: “Importantes modificaciones genéticas en el medioambiente”

Dr. D. Claus Tröger

Día 13 de Noviembre

Tercera sesión: NANOTECNOLOGÍA

Moderador: Dr. D. Sergio Arellano, Chile

08:30h: “Nanopartículas de oro unidas a péptidos para aplicaciones biomédicas”

Dr. D. Marcelo Kogan, CIMAT, Universidad de Chile

09:00h: “Nanotecnología y productos de consumo”

Dr. D. Hernando Gutiérrez Prieto. Profesor Asociado y Co-Director del Centro de Estudios en Bío derecho. Universidad Javeriana-Colombia.

09:30h: “Nanofotónica y sensórica para investigación y desarrollo de biocombustibles”

Dr. D. Beynor Antonio Páez Sierra, Pontificia Universidad Javeriana

10:00h: “La nanotecnología en el Uruguay. Reseña de algunos desarrollos nacionales con aplicaciones biológicas”

Dra. D^a. Helena Pardo, Universidad de Uruguay

10:30h: CAFÉ

11:00h: “Nanomedicina: uso actual y proyecciones”

Dra. D^a. Paola Casanello, Universidad Católica de Chile

11:30h: “Los desafíos para el derecho de seguros planteados por la nanotecnología y sus aplicaciones biológicas”

Dra. D^a. Andrea Signorino Barbat, Universidad de Uruguay.

12:00h: “Pólizas e intermediación de seguros de nanotecnología y nanomedicina”

Dr. D. Raimundo del Río, AON Chile

12:30h: “La liquidación de los nanosiniestros”

Dr. D. Alberto Faraggi Wiehoff, Liquidador, Chile

13:00h: CLAUSURA

Rector de la Universidad Católica de Chile

Dr. D. Rafael Illescas, Presidente de Seaida

Dr. D. Ricardo Peralta Larrain, Presidente de AIDA Chile

Dr. D. Rodrigo Campero, Gerente General de Mapfre Chile

II. NOTAS DE ACTUALIDAD

1. Neutralidad de la Red y Ciberataques

1.1. Consulta pública CE

La CE ha anunciado la apertura de dos consultas públicas sobre Internet, destinadas a defender la "neutralidad" de la red, mediante la ampliación de la libertad de elección de los consumidores sobre operadores y a mejorar la respuesta de la UE ante "ciberataques". Para ello, pide la opinión al respecto de los prestatarios de servicios de Internet fijo y móvil, a los proveedores de contenidos y aplicaciones en red, fabricantes de equipamiento, inversores, asociaciones de consumidores y autoridades públicas.

La consulta servirá para elaborar condiciones que "ampliarán" dicha elección y "pondrán fin a las tergiversaciones sobre la neutralidad de Internet".

La Comisión prevé presentar un conjunto de orientaciones en este sentido en 2013.

La segunda consulta pretende recabar opiniones sobre cómo mejorar la respuesta ante ataques informáticos que puedan dañar el tráfico y la protección de datos en red.

A partir de estas aportaciones, la CE elaborará una propuesta legislativa sobre "seguridad de las redes y de la información" que presentará próximamente, así como un informe de evaluación de los riesgos.

En 2011, los ataques a páginas web crecieron en un 36% en la UE, lo que mantuvo la tendencia al alza de los últimos años, según datos de la Comisión.

1.2. El ciberacoso a través de red alcanza proporciones alarmantes, lo cual ha llevado a diversas modificaciones legales, entre otras conviene destacar el nuevo art.183bis del Código Penal español. El ciberacoso tiene su plataforma más impactante en el denominado “child grooming”, que es un proceso gradual mediante el que una persona establece una relación de confianza con un menor, con abundantes regalos y muestras de amistad y afecto y que poco a poco derivan en un contenido sexual que, por el propio proceso, para el menor se convierte casi en natural y no intimidatorio. Esta figura delictiva existe, con diversas variantes, en varios países.

A efectos del seguro de responsabilidad civil familiar el problema se plantea en lo referente a las medidas preventivas que los padres tienen que adoptar para controlar con quién se relacionan sus hijos por Internet. Son frecuentes los casos tanto de acoso al menor en cuestión como de acoso cibernético de menores a otros compañeros/compañeras, especialmente del mismo colegio, lo que da lugar a una clara responsabilidad de los padres por falta de vigilancia.

A efectos del seguro de rc empresas, tenemos también supuestos claros del uso de ordenador por trabajadores para ciberacosar a compañeras de trabajo, lo cual plantea el problema de la autorización del ordenador para fines privados y de la existencia o no de autorización por parte del patrono.

2. Cloud computing y protección de datos

Informe orientativo del Consejo General de la Abogacía y la Agencia de Protección de Datos.

Los despachos de abogados deben conocer los riesgos que pueden originar el uso de estas tecnologías en su profesión y también en relación con sus clientes, por el secreto profesional y la protección de los datos. Tanto el prestador como el abogado deben actuar diligentemente solicitando y ofreciendo información detallada sobre las medidas que vayan a garantizar la seguridad y confidencialidad de la información.

Las garantías que se deben exigir al prestador de cloud son las siguientes: disponibilidad permanente del servicio y portabilidad de la información, cumplimiento de la legislación nacional e internacional aplicable en función de la territorialidad y específicamente en materia de protección de datos; la asunción de su papel de encargado del tratamiento de ficheros; gestión de las subcontrataciones para el tratamiento de la información; el acceso de los datos; la integridad y conservación de los datos; gestión de copias de seguridad; recuperación ante desastres; continuidad del servicio; consecuencias por incumpliendoos de las obligaciones contraídas.

3. Imágenes digitales mediante sistemas de reconocimiento facial

Análisis de las autoridades europeas

El Grupo de Trabajo del artículo 29 (GT 29) ha aprobado un dictamen sobre el impacto de estos sistemas en servicios y aplicaciones móviles online. Analiza los riesgos para la privacidad, como los posibles tratamientos de imágenes de forma ilegal, las violaciones de la seguridad o la falta de precisión en la identificación. Considera que debe existir un consentimiento previo e informado de los usuarios para llevar a cabo el tratamiento de imágenes digitales a través del reconocimiento facial.

4. Captación de imágenes de Google y protección de datos

Información previa y comprobación de la Agencia de Protección de Datos

Google informó previamente a la Agencia de protección de datos (AEPD) de la captación de imágenes en diversas provincias españolas. La AEPD comprobó que Google había captado, además de datos de localización de sus titulares, datos personales que formaban parte del contenido de comunicaciones, como direcciones de correo electrónico- con nombre y apellidos- mensajes asociados a esas cuentas y a servicios de mensajería, códigos de usuario y contraseñas, entre otros.

5. La responsabilidad civil de los prestadores de servicios por comentarios alojados en sus páginas web

La utilización de las páginas web para comentarios inadecuados, a veces insultantes, por usuarios está proliferando en los últimos tiempos y da lugar a plantearse de nuevo la responsabilidad en que pueden incurrir las empresas que prestan los servicios de páginas webs.

Los prestadores de servicios de alojamiento y almacenamiento de datos, en principio, están en una posición neutra, puesto que solo ponen a disposición de los usuarios la página web. Son los propios usuarios los que dotan a dicha página de contenido, mediante foros o herramientas análogas.

Pero los comentarios vertidos por los usuarios suelen, a veces, dañar el derecho fundamental al honor, a la intimidad personal, familiar y a la propia imagen dando lugar a indemnización de daños y perjuicios.

El prestador del servicio de intermediación que alberga los datos proporcionados por el usuario (art. 16 LSSICE) no responde de dicha información siempre que no tenga conocimiento efectivo de que la actividad o información almacenada es ilícita o lesiona bienes o derechos de terceros susceptibles de indemnización o bien si tienen dicho conocimiento retiran los datos o hacen imposible el acceso a los mismos.

En resumen, no existe una obligación previa de supervisar los comentarios vertidos en la red, no responde en caso de no tener conocimiento efectivo del contenido vejatorio, y si tiene dicho conocimiento por cualquier medio, debe proceder a retirarlo.

III. JURISPRUDENCIA

1. Red Wifi

Sanción por gratuidad a los ciudadanos sin inscripción en el Registro de operadores

Sala de lo Contencioso-Administrativo, sección 8ª, de 1 de septiembre de 2011

La comunicación fehaciente y la inscripción en el Registro de Operadores constituye un instrumento de control de acceso al mercado y la única excepción legal reside tan sólo en que efectivamente concurra la autoprestación del servicio. Por tanto, la CMT impuso a un Ayuntamiento una multa por infracción muy grave al ofrecer y prestar un servicio de proveedor de acceso a internet wifi sin haberse inscrito en el mencionado registro de operadores. Para que estemos ante una auto prestación debe contarse con suficientes garantías o herramientas de que aquel acceso a Internet a páginas o para funcionalidades distintas de las estrictamente vinculadas a los servicios públicos municipales no se produzca.

2. Revelación de secretos de empresa

Apoderamiento de archivos informáticos de empleados

SAP de Sevilla, sección 7ª, de 30 de diciembre de 2011

Dos trabajadores de una consultora laboral que tras cesar en su relación laboral, crean una sociedad de idéntico objeto social con la apropiación de archivos informáticos. En éstos había balances, facturas, libros, escritos dirigidos a determinadas administraciones, resúmenes de estados de tesorería de determinadas sociedades, declaraciones fiscales, contabilidades, contratos, altas y bajas en seguridad social...etc. La AP condena a los acusados por delito de revelación de secretos de empresas.

3. Actualización del concepto legal de divulgación de los nuevos medios de información tecnológica

SAP de Madrid, sección 28ª, de 11 de noviembre de 2011

Relevancia del previo depósito de anterioridades extranjeras en el Fondo documental de la OEPM a los efectos de la divulgación en España para la integración del estado de la técnica en sede de modelos de utilidad.

La sentencia considera la disponibilidad y normal uso de medios tecnológicos utilizados por los expertos en la materia. La existencia de bases de datos de patentes on line como Espacenet (libre, gratuito y muy usual) obliga a una actualización del concepto legal de la divulgación en España en sede de modelos de utilidad, con especial relevancia a la hora de valorar la disponibilidad de anterioridades extranjeras. Las bases de datos de patentes como Espacenet no dejan de ser <<cualquier otro medio>> según la dicción del art. 145.1 de la Ley de Patentes, y como tal ha de valorarse a los efectos de determinar lo divulgado en España en cada casa específico. Ello tiene un impacto en la integración del estado de la técnica en España y la consecuente valoración del requisito de la novedad relativa de los modelos de utilidad.

4. El acceso a la información acumulada en el ordenador

4.1. Facultad del empresario de chequear los correos electrónicos

STSJ de Madrid, Sala de lo Social, Sección 4ª, de 23 de diciembre de 2011

El Letrado socio de una firma en colaboración con otro también de la firma pretendieron la creación de una firma paralela, que una vez en funcionamiento supondría su competencia directa, con la incorporación de 12 abogados del despacho además de colaboradores externos habituales del mismo y personal administrativo. Tales datos se comprobaron a través de averiguaciones realizadas por una empresa informática forense mediante la investigación de los medios electrónicos de comunicación y ordenadores pertenecientes a la Firma de Abogados. No existe vulneración de derecho fundamental, pues la intranet contenía medidas para un buen uso de los recursos informáticos y que se avisaba a la usuarios del correo electrónico que el despacho se reservaba la facultad de chequear los mismos, conforme a la facultad de dirección y control de la actividad laboral que el artículo 20.3 ET atribuye al empresario. La medida es idónea para la finalidad pretendida, necesaria y equilibrada al menos en parámetros constitucionales, por lo que no hay ninguna intromisión al derecho a la intimidad personal consagrado en el artículo 18 CE

4. 2. El acceso a la información acumulada en el ordenador pertenece al ámbito de la intimidad. El acceso no consentido por propietario o por autoridad judicial,

solo es legítimo si existen razones de necesidad y urgencia y se respetan los principios de proporcionalidad y razonabilidad

ST del TC, Sala Segunda, de 7 noviembre de 2011.

El TC se pronuncia afirmativamente en el sentido de que un ordenador personal es un medio idóneo para el ejercicio de la intimidad personal; pueden surgir riesgos considerables por el cúmulo de información acumulada por el titular, entre otros sobre su vida privada y profesional, o cuando el sujeto navega por Internet. El uso de este puede afectar al secreto de las comunicaciones y al derecho a la intimidad personal.

El acceder el encargado del establecimiento de informática a una determinada carpeta (con contenido pedófilo) para verificar la reparación efectuada de la grabadora del ordenador, que carecía de contraseña y sobre lo que se había preguntado al cliente, no supone una extralimitación.

La policía, a denuncia del reparador, procedió a revisar el contenido del ordenador sin autorización judicial; aunque la autorización concedida por el propietario del ordenador al dueño de la tienda no es extensible al posterior acceso de la policía, sin embargo, esta perseguía un fin legítimo, por lo que su actuación fue correcta, necesaria y razonable

4.3. La licitud o ilicitud en el examen del contenido del ordenador de una trabajadora ordenado por el empleador

STS, Sala de lo Social, de 6 de octubre de 2011

La empleada utilizó el ordenador facilitado por la empresa para asuntos propios. La empresa había prohibido de forma tajante la utilización del mismo para cualquier actuación que no fuera la de la realización del trabajo encomendado. La decisión de despedir a la trabajadora fue correcta porque

- el empresario había prohibido de forma tajante el uso para fines distintos a los empresariales, prohibición plasmada por escrito y notificada a todos y cada uno de los empleados
- la monitorización del ordenador de la empleada se hizo por medio de un sistema de software pasivo y poco agresivo que solo permitía captar las pantallas a las que accedían los trabajadores para su posterior visualización y no permitía acceder a los archivos del ordenador protegidos por contraseñas.
- el empresario tiene un poder de dirección empresarial de la actividad de los trabajadores que permite controlar dicha actividad
- los límites a ese control del uso de ordenador vienen establecidos por la posibilidad de respetar el espacio de privacidad consecuencia de la dignidad del trabajador
- sin una previa normativa empresarial acerca del uso del ordenador el empresario no puede entrar de forma lícita en el control del mismo

5. Páginas web y chats

5.1. Utilización y difusión en internet de datos personales sin consentimiento del interesado

SAP de Valencia. Sección 3ª, de 18 de octubre de 2011

La difusión de datos realizada a través de un medio tan expansivo como internet, haciéndolo en una página de contenido sexual, permitiendo el acceso a terceros de esos datos, poniendo de manifiesto un inexistente interés en el titular de los

mismos, supone una intensidad lesiva a la dignidad de la perjudicada, generándole desasosiego y sentimientos de humillación, intensidad que viene revelada por el medio utilizado y forma de hacerlo.

5.2. No vulnera el derecho al honor el decir que “si algo sabe es robar”, que “era una cueva de ladrones” y los integrantes de la institución unos “parásitos”

STS, Civil, 29 de febrero de 2012

Los comentarios, publicados en la página web de un sindicato, se proyectan sobre aspectos de interés público al enmarcarse dentro del conflicto existente entre los partidarios y detractores del cobro por parte de la SGAE de las retribuciones económicas correspondientes a los titulares de los derechos de propiedad intelectual que la misma gestiona.

La gravedad de las expresiones utilizadas no es suficiente para considerar prevalente el derecho al honor frente al derecho a la crítica, teniendo en cuenta el contexto de fuerte discusión existente sobre el tema o también que no se contienen afirmaciones de se aproximen al terreno de la alusión o amenaza personal.

5.3. Difusión en páginas de internet de comentarios y escritos ofensivos para la persona de un médico y para su prestigio profesional

STS, Civil, de 3 de abril de 2012

La demandada difundió a través de la página web toda una serie de expresiones difamatorias referidas al médico y relacionadas con su actuación profesional, comparando la misma con los experimentos llevados a cabo en la Alemania nazi. Se culpaba al médico de la muerte del hijo de la demandada.

La demandada fue condenada por intromisión ilegítima en el derecho al honor del médico mediante la página web, al cese inmediato de la difusión de los contenidos atentatorios a la dignidad, a abstenerse en el futuro de reproducirlos y difundirlos en cualquier medio de comunicación, a dar las instrucciones necesarias a cuantos prestadores de servicios de intermediación sea necesario para el cese de la difusión de dichos contenidos, a los gastos de publicación de la sentencia y al pago de 9.000 euros en concepto de indemnización (el médico había pedido 30.000 euros en concepto de daño moral).

IV. LEGISLACIÓN

1. Página web de la sociedad de capital

Ley 1/2012, de 22 de junio, de simplificación de las obligaciones de información y documentación de fusiones y escisiones de sociedades de capital.

La Ley pretende facilitar el funcionamiento de las sociedades mercantiles y de posibilitar el ahorro de costes, con la potenciación de la página web y las comunicaciones electrónicas; y lo hace incluyendo el régimen jurídico general de la página web y la previsión expresa de esas comunicaciones electrónicas entre la sociedad y los socios. Por lo que se refiere al régimen jurídico general de esa página – que tiene carácter obligatorio para las sociedades cotizadas–, se regula la creación, la modificación, el traslado y la supresión de la misma, se establecen los deberes de los administradores respecto de lo insertado en ella y se disciplinan las cuestiones referentes a la interrupción del acceso. La sociedad garantizará la seguridad de la

página web, la autenticidad de los documentos publicados en esa página, así como el acceso gratuito a la misma con posibilidad de descarga e impresión de lo insertado en ella

2. La mediación electrónica como resolución de conflictos

Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles

Las partes en un procedimiento de mediación pueden acordar que todas o algunas de las actuaciones se lleven a cabo por medios electrónicos, por videoconferencia u otro medio análogo de transmisión de la voz o la imagen, siempre que quede garantizada la identidad de los intervinientes y el respeto a los principios de la mediación.

La mediación sobre reclamación de cantidad se desarrollará preferentemente por medios electrónicos siempre que no exceda de 600 euros. Se prevé la promoción gubernamental de un procedimiento simplificado de mediación electrónica para reclamaciones de cantidad, que no se refieran a confrontaciones de derecho, que tendrá una duración máxima de un mes.
