S

OMPI

SCCR/7/3
ORIGINAL: Inglés
FECHA: 4 de abril de 2002

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL
GINEBRA

COMITÉ PERMANENTE DE DERECHO DE AUTOR Y DERECHOS CONEXOS

Séptima sesión
Ginebra, 13 a 17 de mayo de 2002

ESTUDIO SOBRE LA PROTECCIÓN DE LAS BASES DE DATOS NO ORIGINALES

preparado por el Sr. Sherif El-Kassas,
Director Adjunto del Departamento de Informática del
Campus de El Cairo de la American University

ÍNDICE[*]

Página

[*] A petición de sus Estados Miembros, la OMPI encargó, en el año 2001, la preparación de cinco estudios sobre las repercusiones económicas de la protección de las bases de datos no originales en los países en desarrollo y los países con economías en transición. El presente estudio constituye uno de los cinco estudios encargados y en él consta únicamente la opinión del autor, así como el resultado de sus investigaciones, pero no refleja la opinión ni la postura de la OMPI al respecto.

Página

RESUMEN DEL ESTUDIO

Este documento está centrado en las repercusiones de la protección de bases de datos no originales en los países en desarrollo. Se abordan exclusivamente las bases de datos que no están protegidas en virtud del derecho de autor. Se examinan, concretamente, dos aspectos principales: las repercusiones que podría tener la protección de bases de datos no originales en el desarrollo y alternativas técnicas a la protección jurídica.

En el documento se expone un panorama general de las principales iniciativas que se han tomado en el ámbito de la protección de las bases de datos, a saber: el modelo de la Comunidad Europea, los modelos estadounidense e internacional, y la legislación de México y los países escandinavos. Se procede luego a examinar los principales argumentos a favor y en contra de la protección de las bases de datos no originales. Se pasa también revista a posibles medidas técnicas de protección y a ejemplos de sectores con problemas similares. Por último, se exponen varias conclusiones. El documento va acompañado de apéndices en los que se presenta un panorama más detallado de varias medidas técnicas de protección que se consideran importantes.

Los partidarios de la protección de bases de datos afirman que, entre las finalidades de la protección está la necesidad de "proteger a los autores de bases de datos de la amenaza de una apropiación destructiva del mercado por parte de rivales que se aprovechen de la situación sin ofrecer contrapartida" [1], fomentar las inversiones en la recopilación de determinados tipos de datos y mantener una ventaja equitativa en relación con las empresas de la Comunidad Europea (y otras regiones) que ejercen una protección *sui generis* de las bases de datos y la hacen extensiva a empresas extranjeras sobre la base de un trato recíproco[3].

Ahora bien, hay también quien opina que este tipo de protección "crearía de hecho un sistema exclusivo de derechos de propiedad de una duración prácticamente ilimitada [...]", y que "pondría en peligro la investigación científica de base, suprimiría la competencia en los mercados respecto de productos y servicios con valor añadido y transformaría las actuales barreras de entrada en insuperables barreras jurídicas".

Por consiguiente, en el documento se llega a la conclusión de que la protección *sui generis* de las bases de datos no originales, tal como se propone en la actualidad, repercutiría negativamente en los países en desarrollo y en los círculos científico y académico de todo el mundo. Además, se afirma que a las preocupaciones legítimas de los que compilan bases de datos puede responderse en el marco de la legislación y los sistemas vigentes de propiedad intelectual y mediante medidas técnicas de protección de sus sistemas de bases de datos.

ESTUDIO

I. DESCARGO DE RESPONSABILIDAD

El presente estudio ha sido encargado por la OMPI a fin de tratar de la repercusión de la protección de las bases de datos no originales en los países en desarrollo. El estudio ha de ser utilizado por el Comité Permanente de Derecho de Autor y Derechos Conexos en su labor sobre el posible establecimiento de un instrumento internacional para la protección de las bases de datos.

El estudio trata exclusivamente de las bases de datos que no están protegidas en virtud del derecho de autor (es decir, que no satisfacen el criterio de originalidad del Convenio de Berna y del Tratado de la OMPI sobre Derecho de Autor).

Como el autor del presente estudio posee una formación técnica y cuenta con experiencia en el ámbito de las tecnologías de la información en los países en desarrollo, la seguridad de los sistemas de tecnologías de la información y las aplicaciones de las tecnologías de la información en la administración de los derechos de propiedad intelectual, el estudio se centrará en dos aspectos principales: las posibles consecuencias de la protección de las bases de datos no originales en el desarrollo y las alternativas técnicas a la protección jurídica.

El autor desea mostrar su reconocimiento al Sr. Sherif Saadallah y al Sr. Shakeel Bhatti por su apoyo y por haber dirigido la atención del autor hacia informaciones básicas de calidad inmejorable.

II. INTRODUCCIÓN

Los partidarios de las iniciativas de protección de las bases de datos aseguran que entre los objetivos de la protección figura la necesidad de “salvaguardar a los fabricantes de bases de datos de la amenaza de apropiación por parte de beneficiarios sin contrapartida que actúan como competidores y tienen consecuencias destructivas sobre el mercado,” [1] fomentar la inversión para la recopilación de determinados tipos de datos y mantener una ventaja equitativa en comparación con las empresas radicadas en la CE (y otras regiones) que proporcionan una protección *sui generis* a las bases de datos y la hacen extensiva a las empresas extranjeras sobre la base de un trato recíproco [3].

Las legislaciones sobre bases de datos parecen ofrecer protección a todo aquel que invierta en la recopilación de material y en la elaboración de una base de datos [1,6]. Para lograr la protección no se exige que la base de datos contenga contenido original o constituya una obra original.

Se alega [1] que este tipo de protección, propuesto en las iniciativas de la CE y de los Estados Unidos, “crearía un régimen exclusivo de derechos de propiedad que tendría una duración virtualmente ilimitada y estaría sujeto a escasas limitaciones de política pública, si las hubiere. Así, pondría en peligro la investigación científica de base, eliminaría la competencia en los mercados para los productos y servicios con valor añadido y convertiría las actuales barreras para la entrada de productos y servicios en insuperables barreras jurídicas. Por tanto, es posible que la iniciativa europea y la de los Estados Unidos den lugar a precios relativamente altos por la utilización de bienes públicos. No obstante, en aras de la

eficacia económica, se necesitan unos precios muy reducidos para tales usos, así como unos incentivos mínimos que proporcionen la inversión y los servicios necesarios" (traducción oficiosa).

La naturaleza de los sistemas de información digital también ha contribuido a que existan motivos para proporcionar protección jurídica a las bases de datos. Esto se debe principalmente a la facilidad de acceder a la información digital publicada y de poder copiarla.

Panorama general de las iniciativas de protección de las bases de datos[1]

Se sostiene que las legislaciones sobre derecho de autor excluyen las bases de datos no originales, lo que ha motivado el deseo de llenar el vacío existente entre la mayoría de los sistemas jurídicos actuales en materia de propiedad intelectual y la necesidad de protección de las bases de datos. De aquí surgen las propuestas de proteger "las bases de datos no susceptibles de protección por derecho de autor en virtud de sistemas especiales o *sui generis* de propiedad intelectual que se apartan de los modelos clásicos de protección por patente y derecho de autor subyacentes a los Convenios de París y de Berna" [1].

a) La iniciativa de la Unión Europea

En el contexto de la protección de las bases de datos, se informa [1] de que la Comisión de las Comunidades Europeas persigue dos objetivos: 1) armonizar las normas de los Estados miembros respecto de las bases de datos susceptibles de protección por derecho de autor; y 2) llenar el vacío observado en los regímenes actuales de propiedad intelectual respecto de las compilaciones electrónicas de datos.

La orientación de la Comisión Europea en el sentido de contar con un derecho de propiedad sólido y exclusivo para la protección de las bases de datos rige la Directiva de las Comunidades Europeas sobre bases de datos [1,6].

El derecho *sui generis* otorgado a los fabricantes de bases de datos les permite obtener el derecho exclusivo de "prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de [la base de datos]." Este derecho exclusivo estará vigente durante un período inicial de al menos quince años. El editor de dicha base de datos puede renovar continuamente ese derecho por períodos adicionales de quince años, en caso de que haya efectuado inversiones adicionales en la base de datos.

La Directiva de la CE condiciona la protección *sui generis* a la demostración de que "ha habido una inversión sustancial desde el punto de vista cuantitativo o cualitativo en la obtención, la verificación o la presentación del contenido o en cualquier modificación sustancial que resulte de la acumulación de adiciones, supresiones o cambios sucesivos." Se anuncia que la Directiva de la CE no proporciona directrices para la evaluación del nivel de inversión exigido. Por esta razón, sigue siendo dudoso el nivel exigido para la protección. Además, "no existen límites al número de modificaciones cuantitativas o cualitativas que reúnan los requisitos necesarios para dichas ampliaciones, y cualquier editor que siga

[1] Esta sección se basa en la presentación y el material que figuran en [1,6].

efectuando una inversión sustancial en la actualización, mejora o ampliación de una base de datos existentes puede obtener una protección indefinida" [1] (traducción oficiosa).

De lo anterior se desprende que el derecho *sui generis* depende exclusivamente de la *inversión*. Sin embargo, "el alcance de la protección que la Directiva Final de la CE otorga a los inversores sobre las bases de datos no susceptibles de protección por derecho de autor parece que es el equivalente aproximado al otorgado a los autores de compilaciones no susceptibles de protección por derecho de autor" [1] (traducción oficiosa).

Además, en virtud de la Directiva de la CE, "cada vez que se produzcan datos, aunque sean corrientes o triviales, se obtendrá la protección en caso de que el proceso cueste dinero, y cada nueva producción o reutilización de los mismos datos en actualizaciones, adiciones y ampliaciones que cuesten dinero ampliarán esa protección sin límite de tiempo." (Traducción oficiosa).

En consecuencia, un tercero no podrá evitar el costo de volver a producir los datos ya existentes, salvo que el fabricante original de la base de datos en cuestión la haya abandonado o haya declinado ejercer sus derechos de propiedad, de modo bastante similar a lo que ocurre en virtud del derecho de marcas.

Además, independientemente de que sea posible volver a producir los datos a partir de fuentes disponibles públicamente, quienes invierten en la fabricación de bases de datos siempre podrán denegar a un tercero el derecho a utilizar datos ya existentes en aplicaciones con valor añadido.

Se afirma [1] que la Directiva de la CE no alberga ninguna concepción práctica de dominio público. Fundamentalmente, esto se debe a que gracias a cada nueva ampliación de sus derechos exclusivos, el fabricante de la base de datos (debido a sus inversiones en actualizaciones, adiciones y revisiones) estará en condiciones de recibir la protección de la base de datos en su totalidad por un período adicional de quince años.[2] Esta posibilidad refuerza la capacidad del fabricante original de denegar a terceros el derecho a basarse en conocimientos científicos y técnicos preexistentes y crea otra barrera a la entrada de productos y servicios.

Esto cobra especial importancia en el caso de los países en desarrollo y subdesarrollados que quizás carezcan de los fondos necesarios para pagar el acceso a dichas informaciones. En caso de que no existiera la protección, estas informaciones estarían disponibles para ellos de modo gratuito.

b) El modelo internacional y el de los Estados Unidos

Los Estados Unidos y la Unión Europea han presentado propuestas de protección mundial del contenido de las bases de datos en virtud de regímenes *sui generis* de propiedad intelectual similares a los incluidos en la Directiva de la CE.

---

[2] Esta protección ampliada no se limita al material revisado o añadido, tal y como sucedería en virtud de la legislación sobre derecho de autor.

En diciembre de 1996, la OMPI acogió una conferencia diplomática para considerar estas propuestas. Con arreglo a la propuesta de los Estados Unidos, también se extendía la protección al compilador de los datos. El compilador estaría habilitado para gozar de derechos exclusivos a fin de impedir la extracción y reutilización de la totalidad o de partes sustanciales de una base de datos habida cuenta de que había efectuado inversiones sustanciales en la colección, reunión, verificación o presentación del contenido de la base de datos. En caso de que el compilador continuara invirtiendo en la actualización o mantenimiento de la base de datos, el plazo inicial de protección, de veinticinco años, podría renovarse indefinidamente.

Además, en la propuesta estadounidense figuraba una definición más amplia de base de datos. En ella se incluyen los elementos de programas informáticos no susceptibles de protección por derecho de autor, y no se suministra ningún criterio aparente para la exclusión de hechos o datos compilados para obras científicas e históricas. Además, en la propuesta efectuada por los Estados Unidos a la OMPI, se otorgaría a los fabricantes de bases de datos un plazo inicial de protección de veinticinco años.

La propuesta estadounidense refuerza el aspecto más inquietante de la Directiva de la CE, en el sentido de que impide la formación de un dominio público en evolución a partir del que un tercero pueda obtener datos de manera gratuita.

La propuesta estadounidense, "proporciona un período de protección más prolongado, derechos exclusivos más poderosos, ninguna excepción o privilegio de interés público, severas sanciones penales [...] y normas subsidiarias que refuerzan el autocontrol de las transmisiones en línea, por lo que en la legislación propuesta por los Estados Unidos se otorgaría a los titulares de las bases de datos un monopolio más absoluto que el que procede de la Directiva de la CE" [1] (traducción oficiosa).

c) Legislaciones nacionales

La OMPI ha publicado un estudio de la legislación nacional de sus Estados miembros [6][3]. En el estudio se exponían las disposiciones que conceden la protección jurídica *sui generis* para las bases de datos que no cumplen los criterios de originalidad en los siguientes países: Dinamarca, Finlandia, Islandia, México, Noruega y Suecia.

La protección otorgada bajo las legislaciones nórdicas (Dinamarca, Finlandia, Islandia, Noruega y Suecia) únicamente abarca la copia (en Islandia, la reimpresión y la copia). No se concede protección contra otra utilización y las leyes no especifican la medida en que resultan aplicables en cuanto a la extracción y copias no autorizadas de partes de compilaciones protegidas.

La duración de la protección y el cálculo de la misma difieren ligeramente en las legislaciones nórdicas. En Dinamarca, es de 10 años a partir del año de la primera puesta a disposición del público, pero no excede los 15 años a partir del año de fabricación; en Finlandia, es de 10 años a partir del año de publicación, pero no excede los 15 años a partir del año de fabricación; en Islandia, es de 10 años a partir del año de publicación; y en Noruega y Suecia, de 10 años a partir del año de publicación. Ninguna de estas legislaciones

[3] El resto de este apartado se basa en material extraído de la referencia [6].

contiene disposiciones explícitas relativas a la renovación de la duración en caso de que la compilación se actualice, agrande o revise continuamente o en forma ocasional.

La Ley Federal de Derecho de Autor de México establece una protección *sui generis* de las bases de datos que se extiende a las bases de datos no originales. Los derechos otorgados son los derechos exclusivos a autorizar o prohibir los siguientes actos: 1) la reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma; 2) la traducción, adaptación, reordenación y cualquier otra modificación; 3) la distribución del original o de copias de la base de datos; 4) la comunicación al público; y 5) la reproducción, distribución o comunicación al público de los resultados de las operaciones mencionadas en el apartado 2). El titular original de los derechos es la persona que haya fabricado la base de datos. No existen disposiciones explícitas relativas a la transferencia de la titularidad.

La duración de la protección es de cinco años. No existen disposiciones explícitas relativas a la renovación del plazo en caso de que la compilación sea actualizada, ampliada o revisada en forma continua u ocasional.

III. LOS PRINCIPALES ARGUMENTOS A FAVOR Y EN CONTRA DE LA PROTECCIÓN *SUI GENERIS* DE LAS BASES DE DATOS[4]

a) Los principales argumentos a favor de la protección *sui generis* de las bases de datos

Existen tres argumentos principales que presentan los partidarios de la protección *sui generis* de las bases de datos [2], además de otros argumentos a los que se oponen los países en desarrollo y subdesarrollados. Cabe resumir estos argumentos de la manera siguiente:

1. La considerable inversión en la compilación y mantenimiento de las bases de datos requiere protección adicional. Sobre todo, en el entorno digital y en línea, que hace que sea fácil copiar las bases de datos.

2. La legislación existente sobre derecho de autor no prevé la protección de bases de datos grandes y de carácter general que son utilizadas por medio de un dispositivo de búsqueda. El compilador no ha ejercido ninguna selección puesto que las bases de datos son de carácter general. Además, únicamente se produce la reordenación cuando el usuario lleva a cabo una búsqueda. De ahí que, al no existir ninguna selección o reordenación, no esté disponible la protección por derecho de autor.

3. La Directiva de las Comunidades Europeas sobre las bases de datos proporcionará a las empresas europeas una ventaja en el mercado de bases de datos. Como la Directiva extiende la protección *sui generis* a entidades no europeas con carácter de reciprocidad, en lugar de aplicar el trato nacional, se denegará a las empresas no europeas la nueva protección jurídica otorgada a las bases de datos, a no ser que en sus países de origen se ofrezca una protección comparable.

---

[4] Esta sección se basa en material presentado en las referencias [2] y [3].

4. En los países en desarrollo, la protección puede constituir un motivo para la compilación de bases de datos que pueden tener efectos positivos en el desarrollo (en forma de información que pasa a ser disponible gracias a las colecciones y a la compilación). En otros casos, es posible que la protección contribuya a mantener las inversiones extranjeras.

b) Los principales argumentos en contra de la protección *sui generis* de las bases de datos

Se han expuesto varios argumentos [2. 3] para oponerse a la protección *sui generis* de las bases de datos.

1. Existe una protección adecuada en el actual marco jurídico de la protección intelectual. Por ejemplo, únicamente es necesario que exista una pequeña selección o reordenación para que una base de datos entre dentro del ámbito de protección de la legislación de derecho de autor. Se alega que esto resulta suficiente para proteger a las bases de datos contra la copia en masa.

2. La legislación sobre contratos, secretos comerciales y competencia desleal proporciona un nivel adicional de protección para las bases de datos, independientemente de que la compilación sea susceptible de protección por derecho de autor.

3. Incluso sin protección jurídica, el compilador de la base de datos puede proteger su inversión por medios tecnológicos que impiden copiar la base de datos. Estos medios tecnológicos se reseñan más detalladamente en la sección 4 y en los apéndices.

4. Hasta la fecha no se han presentado pruebas o ejemplos concretos de que un editor de bases de datos haya decidido no desarrollar un producto por temor a que éste reciba una protección insuficiente por medio de la propiedad intelectual. Se afirma que no se han presentado pruebas debido a que éstas no existen [2].

5. El amplio alcance de la protección (previsto en la propuesta de los Estados Unidos) es uno de los puntos más problemáticos. En la propuesta de los Estados Unidos se define a la base de datos como algo que incluye una colección de obras, datos u otros materiales, y esta definición que abarca todo el conjunto de elementos iría más allá de lo que normalmente se considera como base de datos.

6. También resulta problemática la duración de la protección. La Directiva de las Comunidades Europeas ofrece 15 años de protección, mientras que en la propuesta de los Estados Unidos se ofrece una duración de 25 años. Sin embargo, ambos modelos permitirían a numerosas bases de datos recibir una protección ilimitada puesto que cualquier modificación o actualización significativa de la base de datos daría lugar a la creación de una nueva base de datos que gozaría de un nuevo plazo de protección. Esta protección ilimitada, combinada junto con la posibilidad de recibir protección que se aplica a las obras amparadas actualmente por el derecho de autor, podría permitir a los editores de bases de datos eludir los límites impuestos a la protección en la legislación sobre derecho de autor, dando lugar a una drástica disminución del dominio público.

7. Objeciones de científicos e investigadores. La mayoría de las formas de investigación exige la utilización de grandes cantidades de datos, mientras que algunas formas de investigación exigen la utilización de la totalidad de algunas bases de datos. Si las bases de

datos que actualmente están disponibles de manera gratuita entran dentro de la protección *sui generis*, aumentarían de manera inevitable los costos de las investigaciones. Además, la protección *sui generis* impulsará a las instituciones a utilizar sus propias bases de datos como centros de utilidades y por ese motivo tendrá efectos negativos en el intercambio de datos científicos. La protección *sui generis* elevará los costos de las investigaciones y con toda probabilidad hará que resulten prohibitivas para los países en desarrollo.

8. Objeciones de los programadores informáticos. La propuesta de los Estados Unidos trae consigo la posibilidad de que reciban protección las bases de datos contenidas en los programas informáticos. Por consiguiente, los cuadros de consulta, los conjuntos de instrucciones y de caracteres, y las estructuras de datos y elementos de programas similares recibirían protección como bases de datos. Esto obstaculizará el desarrollo de programas informáticos y aumentará los costos, y se trata de otro elemento que cobra especial importancia para los países en desarrollo y que podría impedirles obtener los beneficios de programas de códigos abiertos y gratuitos debido a esta forma de protección.

9. Objeciones de las empresas de Internet[5]. Los cuadros de encaminamiento y los directorios necesarios para el funcionamiento de Internet entran dentro de la definición de base de datos en la propuesta de los Estados Unidos. Por consiguiente, la protección *sui generis* podría dar lugar a la concentración del poder de mercado en Internet. Además, la transmisión no autorizada de una base de datos podría dar lugar a una responsabilidad subsidiaria de la empresa de servicios en línea que proporcionara sin saberlo el material y los programas informáticos mediante los que se llevara a cabo la transmisión. Se trata de otra cuestión importante para los países en desarrollo, puesto que esto dará lugar al aumento de los costos del establecimiento de Internet en las comunidades locales y obstaculizará su difusión.

10. Objeciones de los editores de bases de datos con valor añadido. Existen numerosas empresas legítimas que obtienen datos de las bases de datos existentes y crean valor añadido introduciendo nuevas informaciones o reordenando la información de modo diferente. Cabe la posibilidad de que la protección *sui generis* haga que desaparezca toda esta industria.

11. En los países en desarrollo, las empresas que toman iniciativas para compilar bases de datos sobre los recursos y el patrimonio local pueden llegar a obtener de manera real un monopolio destructivo que es probable que tenga efectos negativos en el desarrollo y el acceso a la información.

IV. ALTERNATIVAS TÉCNICAS A LA PROTECCIÓN JURÍDICA

En la sección anterior se exponen las cuestiones principales relativas a la protección *sui generis* de las bases de datos. El autor cree que dicha protección tendría efectos negativos en el desarrollo. No obstante, es importante no desdeñar el derecho válido de los compiladores de las bases de datos a proteger su inversión. Así, el autor sostiene que en la mayoría de los casos no es necesaria una protección que vaya más allá de la ofrecida por los derechos de propiedad intelectual, de carácter más tradicional, y que en las esferas en las que podía resultar conveniente ofrecer protección adicional pueden desplegarse varias medidas técnicas para llenar el vacío existente.

---

[5] En la referencia [5] figura un tratamiento más detallado de este punto.

a) Sistemas de protección contra la copia

La industria informática ha propuesto numerosos sistemas de protección contra la copia que se utilizan fundamentalmente para proteger el contenido de diversos elementos electrónicos, de multimedios y de datos, entre los que figuran los programas informáticos, la música, los videos y los libros. Los sistemas de protección contra la copia funcionan en el ámbito informativo o en el de los aparatos y pueden emplear soportes lógicos o elementos físicos para lograr sus objetivos. Por ejemplo, la industria del DVD aplica el denominado sistema de aleatorización de contenidos (CSS) para proteger el contenido de los DVD. De manera similar, la industria discográfica trata de fabricar discos compactos protegidos contra la copia que no puedan copiarse fácilmente. En el ámbito de la publicación electrónica, Adobe (*www.adobe.com*), es el creador del programa Acrobat que se ha convertido en norma para la industria. Se trata fundamentalmente de un instrumento para la creación de libros electrónicos y ofrece a los editores que desean proteger su contenido la posibilidad de configurar el programa para limitar la capacidad de los usuarios de reproducir o distribuir sus copias de libros electrónicos. Los editores de bases de datos pueden utilizar los mismos sistemas cuando resulte adecuado; por ejemplo, el editor de un disco compacto que contenga una guía telefónica podrá emplear uno de los sistemas de protección expuestos anteriormente. Gracias a esto el editor tendrá el control sobre la utilización de la base de datos, aunque no estará en condiciones de convertir la base de datos en un monopolio perpetuo. En el Apéndice A se ofrece una reseña de algunos de los sistemas principales que pueden aplicarse directamente al entorno de las bases de datos.

b) Aplicación de dispositivos o programas especiales de visión

Se han propuesto varios sistemas de cifrado para proteger distintos tipos de datos. Por ejemplo, la industria de la radiodifusión viene empleando desde hace tiempo sistemas de cifrado (con distinto éxito) para controlar el acceso a los servicios de televisión de pago. En este sistema el usuario utiliza un dispositivo especial que le permite acceder a la programación de la televisión de pago. El organismo que emite el programa puede controlar fundamentalmente la capacidad del dispositivo de mostrar programas de televisión de pago. Así pues, el organismo de radiodifusión puede proteger sus derechos permitiendo contemplar los programas únicamente a los clientes de pago.

Además, las comunidades del comercio electrónico y de las operaciones de compra y venta de acciones en línea afrontan numerosos problemas parecidos a los que sufre la comunidad de las bases de datos. Esto es especialmente cierto en el caso de la autenticación para el acceso, ámbito en el que dichas comunidades han desplegado sistemas alternativos. Estos sistemas dependen de sólidas técnicas de autenticación que garantizan la identidad de los usuarios de los sistemas mediante el uso de distintas tecnologías criptográficas (en las que se aplican soluciones basadas en soportes lógicos y elementos físicos) para mantener la integridad y seguridad de sus sistemas. En el Apéndice B se exponen los principales problemas, requisitos y medios técnicos de protección existentes en el comercio electrónico. Gran parte de esta experiencia puede utilizarse directamente en el ámbito de la protección de las bases de datos.

Cabe la posibilidad de utilizar sistemas parecidos con las bases de datos en línea. El dispositivo especial utilizado para mostrar la información podría aplicarse a los equipos físicos o a los soportes lógicos (o a una combinación de ambos), lo cual permitiría a los

editores de bases de datos proteger sus derechos sin tener que recurrir a la protección constante, que resultaría excesiva.

V. CONCLUSIONES

Según parece, la protección *sui generis* de las bases de datos está motivada por la idea de que existe la necesidad dentro de la industria de las bases de datos de proteger los esfuerzos y las inversiones realizados en sus productos y actividades comerciales. No obstante, el autor cree que la protección de las bases de datos tendrá efectos negativos importantes en el desarrollo y en el libre lujo de la información en las comunidades científicas.

Las preocupaciones principales reflejadas en el presente documento consisten en quela protección *sui generis* de las bases de datos:

1) menoscabará el dominio público y, por tanto, reducirá de manera significativa la disponibilidad de informaciones y datos gratuitos;

2) puede crear monopolios en perpetuidad que resulten contraproducentes al permitir a los titulares de las bases de datos extender indefinidamente el período de protección;

3) será perjudicial para el libre flujo de información en las comunidades científicas del mundo;

4) será perjudicial para el desarrollo de Internet y de la industria informática puesto que numerosos elementos de los sistemas informáticos pasarán a estar protegidos y de este modo dejarán de estar disponibles para su libre utilización; y

5) obstaculizará numerosos aspectos del desarrollo en los países en desarrollo y subdesarrollados.

Además, el autor sostiene que pueden satisfacerse los intereses legítimos de los compiladores de bases de datos dentro del marco de la legislación y de los sistemas existentes de propiedad intelectual, así como mediante el uso de medidas técnicas similares a las expuestas en los apéndices.

REFERENCIAS

[1] J.H. Reichman y Pamela Samuelson, *Intellectual Property Rights in Data?*, *http://eon.law.harvard.edu/h2o/property/alternatives/reichman.html*

[2] Alan D. Sugarman, *Database Protection–Tilting The Copyright Balance*, *http://www.hyperlaw.com/dbprot1.htm*

[3] Jonathan Band y Jonathan S. Gowdy, *Sui Generis Database Protection: Has Its Time Come?*, D-Lib Magazine, junio de 1997, *http://www.dlib.org/dlib/june97/06band.html*

[4] Anne Linn, History of Database Protection: Legal Issues of Concern to the Scientific Community, *http://www.codata.org/data_access/linn.html*

[5] Gordon Irlam y otros, *Software Developers Comments on the WIPO Database Treaty*, *http://www.base.com/gordoni/thoughts/wipo-db.html*

[6] Legislación Nacional y Regional existente relativa a la Propiedad Intelectual en materia de Bases de Datos, Reunión de Información sobre la Propiedad Intelectual en materia de Bases de Datos, Ginebra, 17 a 19 de septiembre de 1997, WIPO db/im/2. *http://www.wipo.org/eng/meetings/infdat97/db_im_2.htm*

[7] Reunión de Información sobre la Propiedad Intelectual en materia de Bases de Datos, Ginebra, 17 a 19 de septiembre de 1997, *http://www.wipo.org/eng/meetings/infdat97/*

[8] *http://www.wipo.org/eng/meetings/infdat97/db_im_3.htm*

[9] Ross Anderson, *Security Engineering: A guide to building dependable distributed systems*, Wiley, 2001.

[10] Bruce Schneier, *Applied Cryptography*, 2ª edición, Wiley, 1996.

[11] Towards Electronic Commerce in Egypt: A Certificate Authority for Egypt, The Electronic Commerce Committee, The Internet Society of Egypt, CAINET'1998.

APÉNDICE A: SISTEMAS DE PROTECCIÓN CONTRA LA COPIA

Dentro de los sistemas técnicos, las cuestiones relativas al derecho de autor y a la censura guardan relación con el control del acceso, que consiste en limitar el acceso a la información para personas de determinados grupos [9]. Gran parte de los sistemas utilizados corrientemente en el ámbito de la protección contra la copia se pueden utilizar directamente para la protección de las bases de datos.

a) Protección contra la copia de programas informáticos

Entre los principales sistemas de protección de programas informáticos figuran:

– La protección de elementos físicos o dispositivos de clave electrónica que se adjuntan a los sistemas. Es posible copiar el programa informático, pero sin la clave electrónica (un dispositivo resistente a la copia y a la sincronización) el programa no funcionaría.

– La instalación de programas informáticos utilizando métodos resistentes a la copia de originales. Por ejemplo, utilizando una técnica de modificación de sector del disco duro que señalaría un sector concreto de dicho disco como inutilizable, el programa tendría que comprobar dicho sector para garantizar su funcionamiento adecuado.

– La detección del perfil de la instalación física y las pautas de utilización del programa también pueden utilizarse para determinar si el programa está siendo copiado o utilizado por su titular legítimo.

b) Protección contra la copia sonora

La protección por derecho de autor de las grabaciones sonoras es un antiguo problema que data de la década de 1960, cuando se introdujo la grabadora de casetes [9]. En el mundo digital deInte rnet, la protección contra la copia de las grabaciones sonoras pasó a ser un problema importante cuando se hizo popular el formato MP3 de compresión de grabaciones sonoras. Dicho formato permitía a los usuarios comprimir los megaoctetos de las grabaciones de discos compactos en kilooctetos de ficheros MP3 que podían transmitirse por Internet. La industria musical ha intentado dificultar la copia introduciendo formatos alternativos de grabaciones sonoras que incluyen elementos del derecho de autor (utilizando la filigrana digital y técnicas similares).

c) Vídeo y televisión de pago

En el ámbito de las cintas y aparatos reproductores de vídeo hace mucho tiempo que se introdujeron sistemas de protección contra la copia para dificultar la copia o el pirateo del contenido de los videos. Algunos de estos sistemas se basaban específicamente en programas informáticos, es decir, en la manera en que se efectuaba la grabación, mientras que otros dependían del mismo aparato reproductor. La industria de la televisión de pago posee una larga historia de protección del contenido de sus imágenes. La protección adopta normalmente la forma de cajas de adaptación multimedios necesarias para descifrar la emisión televisiva tras su recepción. La industria ha actualizado constantemente los

dispositivos de descifrado a medida que se reducían los costos de la tecnología. A principios de la década de 1970 se utilizaban dispositivos rudimentarios que aplicaban sistemas sencillos basados en simples manipulaciones de las señales televisivas. En la década de 1980, estuvieron disponibles sistemas más complejos (por ejemplo, VideoCrypt y EuroCrypt). Estos sistemas se basaban habitualmente en tres elementos: 1) servicios de gestión por suscripción; 2) cajas de adaptación multimedios; y 3) tarjetas con microcircuitos que contienen las credenciales y la lista de programas de los suscriptores.

d) Disco versátil digital (DVD)

Las normas del DVD (denominado originalmente videodisco digital) son compatibles con el denominado sistema de aleatorización de contenidos (CSS). Los aparatos de DVD utilizan una aplicación incorporada de CSS que presta asistencia al sistema de protección contra la copia. Sin embargo, cabe observar que el sistema aplicable al DVD no ha tenido demasiado éxito ante los intentos de copia. No obstante, aquí se trata de resaltar que cabe utilizar sistemas de naturaleza similar, pero más sólidos, para la protección de las bases de datos.

APÉNDICE B: LOS SISTEMAS DE SALVAGUARDIA DEL COMERCIO ELECTRÓNICO Y SU APLICACIÓN A LA PROTECCIÓN DE LAS BASES DE DATOS

Los sistemas del comercio electrónico comparten la mayoría de los objetivos de la comunidad de las bases de datos (en línea) en cuanto a la protección de sus inversiones y a la integridad de sus sistemas. En el presente Apéndice se subrayan algunos de los principales sistemas tecnológicos utilizados para la obtención de esos objetivos.[6] El autor sostiene que cabe utilizar medios parecidos para obtener una protección tecnológica adecuada de los sistemas de bases de datos.

a) Requisitos y salvaguardias para el comercio electrónico

La seguridad es un requisito fundamental para el comercio electrónico, algo que resulta especialmente cierto en el comercio electrónico que se realiza en una red abierta y poco fiable como Internet. En la presente sección se exponen varios aspectos importantes de la seguridad: los requisitos y las salvaguardias.

i) Requisitos

En general, se pueden establecer cinco requisitos principales de seguridad para el comercio electrónico: 1) autenticación de la entidad; 2) integridad del mensaje; 3) imposibilidad de rechazo; 4) mecanismo de verificación eficaz y 5) confidencialidad.

ii) Autenticación de la identidad

Es necesario autentificar la entidad para garantizar la confianza y las transacciones electrónicas. El objetivo consiste en garantizar que cada parte involucrada en una transacción sea quien afirme ser, es decir, evitar el fraude que pueda surgir como consecuencia de que un impostor se haga pasar por una institución financiera o un comerciante autorizado.

iii) Integridad del mensaje

Es necesario garantizar la integridad del mensaje para evitar errores que puedan surgir debido a cambios en el mensaje durante la transmisión. Dichos cambios pueden ocurrir debido al fraude o al error en el sistema de transmisión.

iv) Imposibilidad de rechazo

Este apartado se refiere a la capacidad de los sistemas de incorporar firmas innegables. Es decir, una vez que una parte determinada ha dado su consentimiento a la transacción, la prueba exigida hace que sea imposible que esta parte niegue su participación en la transacción.

---

[6] El material contenido en el presente Apéndice se basa en la presentación y el material de la referencia [11].

v) Verificación eficaz

Debe de establecerse un mecanismo de verificación eficaz que ha de utilizarse en caso de que surjan controversias, así como para el análisis.

vi) Confidencialidad

La confidencialidad es un requisito corriente para la mayoría de las transacciones financieras, independientemente de que sean electrónicas. Los sistemas electrónicos deben poseer la capacidad de garantizar el anonimato de todas las partes involucradas en las transacciones y la confidencialidad del contenido de la transacción.

vii) Salvaguardias y mecanismos de seguridad corrientes

Para garantizar que se satisfacen los requisitos de seguridad expuestos anteriormente, se deben emplear las salvaguardias y los mecanismos adecuados. En el mundo virtual de los sistemas y redes informáticos las soluciones se basan en el dominio de la criptografía.

viii) Criptografía

La criptografía es la ciencia de la creación de criptosistemas (también denominados sistemas de cifrado). Los criptosistemas son métodos de transformar mensajes de manera tal que únicamente determinadas personas puedan deshacer la transformación y recuperar el mensaje original. Los mensajes se transforman habitualmente utilizando lo que corrientemente se denomina *clave*. Las claves son los instrumentos básicos para abrir y cerrar el sistema de acceso a los mensajes.

ix) Criptografía de clave pública

Al considerar los criptosistemas que se utilizarán en las comunicaciones seguras en una red insegura, como Internet, a menudo hay que basarse en los denominados criptosistemas de clave pública. Dichos criptosistemas utilizan dos claves para solucionar el problema del transporte de la clave. Una de las claves, denominada clave pública, se utiliza para impedir el acceso o cifrar el mensaje, mientras que la otra clave, denominada clave privada, se utiliza para dar acceso o descifrar el mensaje. A fin de establecer comunicaciones seguras utilizando dicho sistema, las dos partes que deseen comunicarse deben enviarse sus claves públicas. Una vez que se han intercambiado las claves, el remitente utilizará la clave pública del receptor para cifrar el mensaje que ha de enviar, mientras que el receptor utilizará la correspondiente clave privada para descifrar el mensaje y recuperar el texto original.

Los criptosistemas de clave pública también pueden utilizarse para crear firmas criptográficas. Una firma criptográfica es un código digital creado utilizando una clave privada y el mensaje que ha de firmarse. Los métodos utilizados para crear la firma se conciben de manera tal que garantizan que cada firma es exclusiva de la clave y de la combinación de mensajes dados. La firma puede comprobarse y verificarse utilizando la correspondiente clave pública.

x) Certificados criptográficos

La criptografía y los sistemas de firma de clave pública satisfacen la mayoría de los requisitos de seguridad expuestos anteriormente. Queda pendiente la cuestión de la autenticación de la clave pública. Esto se debe a que la simple utilización de sistemas de clave pública no garantiza la identidad del titular de la clave. En un sistema incontrolado cualquiera podría publicar una nueva clave pública y asumir una nueva identidad, lo que sería algo parecido a expedir su propio pasaporte o permiso de conducir. Esto resulta claramente inaceptable para cualquier aplicación para la que, como en el caso del comercio electrónico, son necesarias la autenticación y la imposibilidad del rechazo.

Con el fin de resolver este problema (fundamentalmente un problema de confianza) no se permite a los participantes en el comercio electrónico utilizar un par de claves pública y privada. En lugar de ello, deben utilizar claves que estén certificadas por un tercero en quien confíen ambas partes. Habitualmente se hace referencia a dicho tercero como la *entidad certificadora*.

b) Entidades certificadoras

Se considera a la entidad certificadora[7] como el suministrador de la autenticación e infraestructura de seguridad necesarias para garantizar unas comunicaciones más seguras en Internet, lo que hace que ésta sea más adecuada para el comercio electrónico. La entidad certificadora crea y expide certificados que contienen la información necesaria para identificar plenamente a un tercero. Esto se logra incluyendo la información para la identificación de la persona y la clave pública en un paquete, que es firmado por la entidad certificadora.

El hecho de que la entidad certificadora firme el paquete permite a los participantes en el comercio electrónico verificar su validez. Esto es posible debido a que se da por supuesto que todos los participantes conocen la entidad certificadora y confían en ella.

Protocolos de autenticación

La mayoría de los protocolos de autenticación modernos se basan en la criptografía de clave pública y dependen de la asistencia de una entidad certificadora. Varios de dichos protocolos se utilizan en Internet para asegurar la transmisión de mensajes en general, así como para el comercio electrónico.

Entre los ejemplos de protocolos que aseguran la transmisión de mensajes en general figuran los siguientes:

– El protocolo SSL, abreviatura de “capa de zócalos segura”, elaborado inicialmente por Netscape. El SSL puede utilizarse para asegurar cualquier comunicación de aplicaciones en la que se utilice el TCP/IP. Se utiliza con bastante frecuencia para establecer conexiones seguras en línea entre navegadores y servidores de Internet. El SSL y su nueva versión, el TLS, forman parte en la actualidad de los protocolos normalizados de Internet.

[7] En la actualidad se utiliza corrientemente en el marco de una infraestructura de clave pública más desarrollada.

– El protocolo S/MIME, abreviatura de seguras/extensiones multipropósito del correo Internet. Como sugiere su nombre, el S/MIME comprende una serie de especificaciones que permiten a los usuarios intercambiar de manera segura mensajes electrónicos en Internet.

[Fin del documento]