REGULACIÓN DE LAS MEDIDAS TECNOLÓGICAS EN EL DERECHO COMPARADO. ESPECIAL REFERENCIA AL CASO DE ESTADOS UNIDOS, REINO UNIDO Y AUSTRALIA

JUAN SEBASTIÁN SERENO RESTREPO*

SUMARIO

I. Introducción. A. Función práctica de la regulación sobre medidas tecnológicas de protección. B. Breve reseña de la evolución legislativa sobre la materia. II. Estructura regulatoria. A. Medida de protección tecnológica. Concepto y elementos. 1. Producto, dispositivo o componente. 2. La medida debe ser aplicada a un bien inmaterial sujeto al *copyright*. 3. Especial finalidad a la que debe estar afectada la medida tecnológica aplicada sobre la obra: la prevención o inhibición de infracción al *copyright* o el control de acceso a la obra. a. La prevención o inhibición de infracciones al *copyright*. b. El control de acceso a la obra. 4. La medida debe ser efectiva en el control del acceso o en la prevención o inhibición de la infracción de los derechos del titular de la obra. 5. Sujeto calificado para aplicar la medida sobre la obra protegido por el *copyright*. B. Consecuencias jurídicas de la elusión. C. Extremos subjetivos. 1. Titular del derecho a la reparación. 2. Sujetos pasivos de la prohibición de elusión y del derecho a la reparación. III. Infracción de la prohibición de elusión de la medida. A. Elusión efectiva de una medida tecnológica ("*anti-circumvention provision*"). 1. La conducta: elusión de la medida. Alcance. 2. Conocimiento de (o deber razonable de conocer) que con la acción se elude una medida tecnológica de protección. B. Conductas respecto de un dispositivo de elusión ("*anti-trafficking provisions*"). 1. Realización de una o varias de las conductas definidas en la ley. 2. Afectación de los dispositivos a una finalidad específica señalada en la ley. 3. Elemento subjetivo. Conocimiento por parte del agente de que el objeto es un dispositivo de elusión de una medida tecnológica de protección.

* Investigador del Departamento de Propiedad Intelectual de la Universidad Externado de Colombia y miembro del Grupo de Investigación en Comercio Electrónico del Departamento de Derecho de los Negocios de la misma universidad. Las opiniones expresadas en este artículo son del autor y, por lo tanto, no comprometen ni responsabilizan a la universidad ni a ninguna otra entidad con la que el autor tenga vínculos. Fecha de recepción: 12 de agosto de 2009. Fecha de aceptación: 11 de septiembre de 2009.

C. Prestación de servicios. IV. Eximentes de responsabilidad por elusión de una medida tecnológica. V. Conclusiones

El cometido de este artículo es analizar los elementos estructurales de la regulación de las medidas tecnológicas de protección en el derecho comparado, especialmente en las legislaciones estadounidense, inglesa y australiana. Para tal fin me valdré, principalmente, de reciente pronunciamientos jurisprudenciales de las cortes de los citados países. Todo lo anterior sin perjuicio de mis opiniones o de comentarios doctrinales o jurisprudenciales de tradición de derecho de autor que puedan ser útiles.

El artículo aborda los tres principales elementos del supuesto de hecho de la regulación de las medidas tecnológicas y su elusión. El primero es el relativo a *qué se debe entender* por una medida tecnológica de protección y *qué condiciones* debe cumplir para que sea jurídicamente tutelada. El segundo es el relativo a las *modalidades de infracción* de las medidas tecnológicas. El tercero trata sobre las *limitaciones y excepciones* a la responsabilidad derivada de la elusión de la medida tecnológica.

El escrito se desarrolla de la siguiente manera: en la introducción se tratará una breve reseña del desarrollo legislativo de la materia y cuál es la función práctica que cumple, en principio, una regulación sobre ella; la segunda parte desarrolla tres temas: *qué debe entenderse* por medida tecnológica de protección y *qué condiciones* debe poseer para que sea jurídicamente tutelada; las *modalidades de infracción* de las medidas tecnológicas y las *limitaciones y excepciones* a la prohibición de –y a la responsabilidad por– eludir medidas tecnológicas.

I. INTRODUCCIÓN

A. FUNCIÓN PRÁCTICA DE LA REGULACIÓN SOBRE MEDIDAS TECNOLÓGICAS DE PROTECCIÓN

Desde el punto de vista de la regulación positiva de la materia, las medidas tecnológicas de protección pretenden ofrecer una solución al problema de garantizar los derechos del titular de la obra en el contexto de los nuevos avances tecnológicos.

Si bien los avances tecnológicos "proporcionan unas herramientas más sofisticadas para la creación y difusión legítimas de obras"[1], también es cierto que "proporcionan herramientas más sofisticadas para la creación y difusión ilegítima de obras"[2].

Son avances tecnológicos significativos que han puesto en peligro los derechos de los propietarios de contenidos: la copia digital, la compresión, la creciente

1. Dean S. Marks y Bruce H. Turnbull. Documento OMPI. *Las medidas tecnológicas de protección: el punto de encuentro de la tecnología, el derecho y las licencias comerciales*, s. d., p. 2.
2. Ídem.

anchura de banda y las conexiones en redes. Todos ellos han dado lugar a que no haya necesidad de "piratas dedicados que usen un equipo caro para copiar obras, ni canales físicos de distribución (desde mercados de baratijas a la venta por esquinas o los comercios al por menor) para distribuir copias no autorizadas. Actualmente, un consumidor individual con algunos miles de dólares invertidos en un equipo para su casa puede crear y distribuir un número ilimitado de copias de obras no autorizadas y de gran calidad"[3].

La copia digital, a diferencia de la analógica, implica la "reproducción bit a bit. Esto significa que cada copia es perfecta, y que se pueden hacer copias perfectas a partir de otra copia y así hasta el infinito. Además, las copias digitales se pueden hacer con gran velocidad y sin sufrir ninguna pérdida de calidad"[4].

La compresión por medio de tecnologías como el MPEG2 para el video y el MP3 para la música ha dado lugar a una reducción considerable en el tiempo y en el ancho de banda necesarios para transmitir la música y el video a través de Internet. En síntesis, "[e]stos adelantos enormes de la tecnología de compresión significan que la transmisión de obras audiovisuales [y musicales] íntegras de alta calidad por redes como Internet resultará cada vez más sencilla, rápida y práctica"[5].

Los adelantos en materia de anchura de banda (módem para cable y líneas de teléfono ADSL de alta velocidad) facilitan y facilitarán "enormemente la distribución de obras con una calidad excepcional a muchas personas en poco tiempo y con un coste reducido"[6].

La creciente conexión en red entre los dispositivos domésticos y entre el hogar y el mundo exterior (y viceversa) permite "que los usuarios reciban y manden obras desde casa y, al mismo tiempo, que pasen obra de un dispositivo a otro en sus hogares […] Todas estas conexiones hacen que para los no profesionales resulte sencillo hacer y distribuir múltiples copias de gran calidad […]"[7].

Las medidas tecnológicas pretenden neutralizar los peligros que los avances tecnológicos crean a los derechos del titular de la obra[8]. Sin embargo, tales medidas

3. Ídem.
4. Ídem.
5. Ibíd., p. 3.
6. Ídem.
7. Ídem.
8. "Para describir el desconcierto provocado por la tecnología digital se ha recurrido a la plástica imagen de la doble pesadilla. De un lado, la de los titulares de derecho […] En principio, la tecnología digital dibuja un prometedor paraíso para ambos. Los titulares de derechos vislumbran el acceso a un público más extenso y sin necesidad de intermediario. Sueñan con un mundo en el que los soportes físicos, las imprentas y otras máquinas, los costes de almacenamiento y distribución, las librerías y otros comercios e incluso las bibliotecas podrían llegar a desaparecer, eliminadas por el formato digital y la relación directa con el consumidor. En lo mejor del sueño, sin embargo, les asalta una pregunta inquietante: si traslado las obras al forma digital ¿Cuántas venderé?... La respuesta, obvia, adquiere tientes de pesadilla: una sola, pues, a partir de ahí, cualquiera podrá copiarla y difundirla libremente. Para evitar que sus temores se vuelvan reales, los titulares han puesto sus esperanzas en la propia tecnología que así sería, a la vez, problema y solución.- La forma de mantener el control en el mundo digital, piensan, pasa por el empleo de medias tecnológicas o candados que permitirán impedir o controlar el

por sí solas son una respuesta limitada e insuficiente en especial por su vulnerabilidad a los ataques de los piratas.

Tal dificultad y otras llevaron a los propietarios de contenidos a afirmar la necesidad de crear normas jurídicas que respalden las tecnologías de protección[9].

b. breve reseña de la evolución legislativa sobre la materia

Las primeras respuestas jurídicas concretas fueron los tratados OMPI de 1996: uno sobre derecho de autor y otro sobre interpretación o ejecución y fonogramas. El primero dispone de manera clara en su artículo 11:

> Las partes contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Berna, y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la ley.

Sin embargo, la prohibición tiene importantes antecedentes en normas de legislaciones nacionales. Vale mencionar algunas de ellas.

En Europa se encuentran, al menos, dos antecedentes. En el Reino Unido, la sección 296 del Copyright, Designs and Patents Act de 1988 prohibía la elusión de mecanismos anticopia aplicados sobre copias de obras en una forma electrónica[10].

acceso y la realización de copias […]": Ramón Casas Vallés. "Copia privada y medidas tecnológicas: el caso 'Mulholland Drive' ", en *Derecho de Autor*, Cerlac-Unesco-Univesidad de los Andes, n.º 1, enero-junio de 2007, p. 206.

9. "Las medidas tecnológicas de protección necesitan un apoyo jurídico y legislativo adecuado, en primer lugar, para asegurar que se respeten dichas medidas, y en segundo lugar, para disuadir la anulación de estas medidas por parte de personas que, de otro modo, infringirían los derechos de los propietarios de contenidos": Marks y Turnbull. Documento ompi…, cit., p. 6. "La apuesta de los titulares pro las medidas tecnológicas de poco valdría si éstas a su vez, no obtuvieran protección legal específica. La orgullosa tecnología a la postre también ha de llamar a las puestas del derecho, impetrando su tutela. *Nihil novum sub sole*. También las tradiciones tecnologías de protección de la propiedad hicieron el mismo recorrido. Una puerta con una simple cerradura, incluso una modesta ventana, son medias tecnológicas que protegen el interior de las viviendas. Pero de bien poco servirían si la ley, en concreto la ley penal, no sancionase con especial dureza a quien entran en ellas forzando tales medidas. Esta es la razón por la cual muy pronto los titulares exigieron –y obtuvieron– una tutela específica de las medidas tecnológicas. Aparte de lo que pueden prever las leyes nacionales, éste fue uno de lo objetivos de los *Tratados Internet* de la ompi y, en el ámbito regional [Europeo], de las Directivas europeas sobre programas de ordenador, y sociedad de la información": Casas Vallés. "Copia privada y medidas tecnológicas: el caso 'Mulholland Drive'", cit., p. 208.

10. "The use of spoilers to prevent copying, for instance of sound recordings and prerecorded computer programs, has been undermined by the production of devices to circumvent such spoilers. Therefore, in an attempt, it would seem, to go away to stopping this activity, section 296 has been included in the 1988 Act. This section applies where copies of a *copyright* work are issued to the public, by or whit the licence of the *copyright* owner, in an electronic form which is copy-protected. Copy-protection includes any device of means intended to prevent or restrict copying of a work or to impair the quality of copies made": Copinger & Skone James. *On Copyright*, x ed., Sweet and Maxell, 1989, p. 825.

La directiva europea del 14 de mayo de 1991 sobre protección de *software* prohibió la elusión de dispositivos anticopia aplicados sobre programas de computador.

En Estados Unidos se encuentran también dos importantes antecedentes. Por un lado, el US Audio Home Recording Act de 1992, que creó la obligación a los productores de equipos de grabación de audio de incluir en sus equipos una medida tecnológica conocida como *serial copy management system* (SCMS), cuya función consiste en evitar que de la copia realizada se puedan realizar copias sucesivas[11]. Por último, la provisión de medios para lograr la copia de obras protegidas por *copyright* ya se hallaba prohibida por vía de *case law* en Estados Unidos, y como subregla especial de esa prohibición –en opinión de una respetada autora de la materia–, la provisión de medios para la elusión de medidas tecnológicas aplicadas para evitar la copia también se hallaba proscrita[12].

11. Para una explicación completa del *video home taping* y del *audio home taping* (a la luz del *fare use*) y del contenido de audio Home Recording Act, ver: ROGER E. SCHECHTER y JOHN R. THOMAS. *Intellectual property the law of copyrights, patents and trademarks*, Thomson-West, 2003, pp. 235-238.

12. PAMELA SAMUELSON señala: "The U. S. could have asserted that its law already complied with the WIPO treaty's anti-circumvention norm. […] The U. S. could have pointed to a number of statutes and judicial decisions that establish anti-circumvention norms": "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", publicado originalmente en 14 *Berkeley Technology L. J.* 519, 521 & 531-32, 1999, p. 14, disponible en [http://people.ischool.berkeley.edu/~pam/papers/Samuelson.pdf]. Puntualmente cita el caso *Sega Enterprises, Ltd. v. Maphia*, 857 F. Supp. 679 (N. D. Cal. 1994). La decisión trataba sobre la concesión de una *preliminary injuction* ordenada el caso de una demanda por infracción de *copyright*, marca y competencia desleal interpuesta por Sega (compañía productora de videojuegos) contra Maphia y otros (empresa dedicada al negocio de *los Bulletin Board* y actividades relacionadas). Tal como se explica en la decision, un *Bulletin Board* "[…] consists of electronic storage media, such as computer memories or hard disks, which is attached to telephone lines via modem devices, and controlled by a computer […] Third parties, known as 'users', of electronic bulletin boards can transfer information over the telephone lines from their own computers to the storage media on the bulletin board by a process known as "uploading." Uploaded information is thereby recorded on the storage media. Third party users can also retrieve information from the electronic bulletin board to their own computer memories by a process known as 'downloading'. Video game programs, such as Sega's video game programs, are one kind of computer programs or information which can be transferred by means of electronic bulletin boards […]". Maphia poseía un *Bulletin*; respecto de lo que interesa aquí, en el caso se demostró que Maphia promocionaba y vendía a sus usurarios un dispositivo llamado *video game copiers* o *super magic drive*, mediante el cual se podía copiar el videojuego contenido en la memoria ROM insertada en el cartucho de los videojuegos de Sega. Así mismo, Maphia incitaba a sus usuarios a cargar los juegos copiados en el *Bulletin* y a descargarlos –para realizar esto último, muchas veces solicitaba a los usuarios el pago de un precio o el intercambio por otros programas o servicios–. Partiendo de que las copias realizadas al cargar y descargar los videojuegos de Sega del boletín son infractoras, y de que tal actividad es facilitada y promocionada por Maphia, la Corte del Distrito de California consideró que tal hecho tiene altas posibilidades de constituir una infracción por vía de *contributory infringement* (una de las dos formas posibles de infracción indirecta según el *case law* de ese país). Como se ve, este caso explícitamente no trata sobre responsabilidad por elusión de medidas tecnológicas. La interpretación dada por la profesora SAMUELSON parece ser la de que este caso prohíbe, so pena de reparar perjuicios, facilitar a terceros la remoción y copia de *software* protegido por *copyright*, y en ese sentido, la prohibición de proveer mecanismos para eludir medidas tecnológicos encaminadas a prevenir la copia sería uno de los eventos comprendidos en esa regla ("*finding copyright liability for providing tools to enable game software to be removed from disks and posted on the Internet*" –pie de página

El siguiente paso fue la incorporación de los mencionados tratados en las legislaciones internas[13]. En Estados Unidos, el Digital Milenium Copyright Act (DMCA, 1998) dispuso en la s. 1201 una prohibición general de eludir medidas tecnológicas, de realizar ciertos actos en relación con dispositivos con aptitud de elusión y de prestar servicios con tal aptitud[14].

La estructura regulatoria estadounidense o al menos sus elementos más relevantes han sido transportados a las legislaciones internas de otros países por vía de tratados de libre comercio[15] y, aunque en este momento no parece muy claro, Colombia podría sufrir este mismo proceso[16].

66 de la página 14 del texto de SAMUELSON). Tal conclusión tiene mayor peso al tener en cuenta que, en el caso concreto, Sega fijaba sus videojuegos en una memoria ROM (*read only memory*), que está diseñada para contener el juego y no permitir posteriores grabaciones ("*Sega's game system is designed to permit the user only to play video game programs contained in Sega cartridges. The system does not permit the copying of video game programs* […]": *Sega Enterprises, Ltd. v. Maphia, 948 F. Supp. 923* [N. D. Cal. 1996]). Que Maphia vendiera a sus usuarios dispositivos con la capacidad de eludir la propiedad de no permitir copia de las memorias ROM constituye, en ese sentido, la provisión de un dispositivo de elusión.

13. MARKS y TURNBULL señalan tres puntos de discusión que deben ser resueltos por las legislaciones: "i) si la prohibición [de elusión de medidas tecnológicas] debería aplicarse tanto a los dispositivos como a los comportamientos; ii) si se debería exigir que los equipos respondiesen a unas medidas de protección particulares; iii) cuáles son las excepciones apropiadas a la prohibición del acto de elusión". Yo agrego un punto, y es el de si deben crearse excepciones no sólo al acto de elusión, sino también a las conductas relativas a dispositivos y servicios de elusión.

14. Para un interesante análisis sobre la constitucionalidad de la s. 1201 (respecto de la prohibición de comercializar dispositivos de elusión de medidas tecnológicas que efectivamente protegen los derechos del autor) frente a la libertad de expresión (Primera Enmienda) y a la competencia del congreso para expedir tal regulación bajo *Intellectual Property Clause*, ver *United States v. Elcom Ltd, 203 F. Supp.2d 1111* (N. D Cal. May 8, 2002).

15. "A key part of the United States' intellectual property trade agenda is securing legal protection against circumvention of technological measures added to *copyright*ed works, based on the provisions in the U. S. Digital Millennium *Copyright* Act (DMCA). Anti-circumvention provisions based on those in the DMCA have been included in the IP chapters of the bilateral free trade agreements (FTAs) that the U. S. has recently concluded with Jordan (Article 4[13]), Singapore (Article 16.4[7]), Chile (Article 17.7[5]), CAFTA (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic) (Article 15.5[7]), Australia (Article 17.4[7]), Morocco (Article 15.5[8]) and Bahrain (Article 14.4[7]). In addition, Article 22 of subsection B.2.c of the third draft of the IP Chapter of the Free Trade Area of the Americas Agreement also requires signatories to provide legal sanctions for circumventing technological measures added to protect *copyright*ed Works": GWEN HINZE. "Seven Lessons from a Comparison of the Technological Protection Measure Provisions of the FTAA, the DMCA, and recent bilateral Free Trade Agreements, Documento de Electronic Frontier Foundation", en [www.eff.org/pages/seven-lessons-comparison-technological-protection-measure-provisions]. "Since the passage of the DMCA in 1998, the United States has included language that parallels the anti-circumvention provisions of the DMCA in trade pacts. […] Similar provisions are in the trade agreements with Australia, Bahrain, Chile, Morocco, Oman, and Singapore, *as well as one being negotiated with Colombia*, Ecuador, and Peru": LEE HOLLAAR. *A Bad Trade - Will Congress Unwittingly Repeal the Digital Millennium Copyright Act and Violate our Trade Treaties?*, Institute for policy Innovation, Center for Technology freedom, 2006, p. 5 (cursivas agregadas).

16. NICK TIMIRAOS. "Obama Vows Opposition to Colombia Trade Deal", en *The Wall Street Journal*, 4 de abril de 2008, en [http://blogs.wsj.com/washwire/2008/04/02/obama-vows-opposition-to-colombia-trade-deal/?mod=wsjblog]; "Cámara de Representantes de

Otros países también han adaptado su legislación interna a lo requerido por el artículo 11 del convenio. Para efectos de este escrito, interesa mencionar que tal proceso se dio en el Reino Unido en 2003 y en Australia en 2006.

El colofón de lo hasta ahora dicho es que la legislación (internacional y nacional) que prohíbe actos que efectiva o potencialmente resulten en elusión de las medidas tecnológicas de protección tiene la función práctica, en principio, de reforzar y respaldar la protección parcialmente otorgada por las medidas tecnológicas a los derechos de los propietarios de contenidos en el nuevo entorno digital, que ofrece amplias posibilidades para la reproducción (de alta calidad y cada vez menor tamaño) y distribución (cada vez más rápida y con vocación global) prohibida[17].

II. ESTRUCTURA REGULATORIA

Explicada la función práctica de las medidas tecnológicas de protección, la de su regulación y la evolución legislativa de la materia, es hora de estudiar la normatividad. Tal tarea es la que se ha de desarrollar a continuación.

A. MEDIDA DE PROTECCIÓN TECNOLÓGICA. CONCEPTO Y ELEMENTOS

De un ejercicio de derecho comparado surge el concepto de medida tecnológica de protección o *technological protection measure* (TPM) como *cualquier dispositivo, producto o componente diseñado para prevenir o inhibir, en el curso normal de su operación, la infracción del* copyright *sobre una obra o para controlar el acceso a ella*. Esta definición es la pieza principal del supuesto de hecho de la normatividad que se estudia.

EE. UU. deja en el limbo discusión del TLC", 10 de abril de 2008, en [www.elespectador.com/noticias/negocios/articulo-camara-de-representantes-de-eeuu-deja-el-limbo-discusion-del-tlc].

17. Quiero aclarar desde ahora la aceptación de la necesidad, la conveniencia y la forma de desarrollar una regulación de la materia no es un asunto en el que haya consenso. Algunos han expresado su preocupación respecto de los efectos que sobre la economía digital, el uso legítimo de las obras y la libertad de expresión puede tener esta regulación. Para más: SAMUELSON. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", cit. En el sistema de derecho de autor, consúltese el ilustrativo caso francés del *Mulholland Drive* (y sus respectivos comentarios doctrinarios) sobre los conflictos que pueden surgir entre la utilización de medidas tecnológicas y las limitaciones y excepciones al derecho de autor en CERLAC-UNESCO-UNIVERSIDAD DE LOS ANDES. *Derecho de Autor*, año 1, n.º 1, enero-junio de 2007, pp. 192-233. Otros apoyan la legislación antielusión y critican a quienes acusan a tal legilación por supuestos efectos dañosos: "It might be worth trying to change, or even dumping, those trade agreements if the anti-circumvention provisions of the DMCA, and in particular the trafficking provisions and the circumvention to access provision effectively repealed if H. R. 1201 becomes law, were causing real problems. But it appears that they are not. […] While it may be argued that those reports are just the tip of the iceberg, and that people are not innovating because they are concerned about violating the DMCA anti-circumvention provisions, it is more likely that any chilling comes from the overheated rhetoric of the DMCA opponents who use it as a boogie man to get people to support their calls for repeal, and not what has actually happened since the enactment of the DMCA in 1998.": HOLLAAR. *A bad trade*… cit., (p. 5-6).

El concepto de medida tecnológica de protección puede descomponerse en los siguientes elementos:

1. Producto, dispositivo o componente

¿En qué se concreta una medida tecnológica de protección tutelada jurídicamente? La respuesta a esta pregunta determina de manera radical el ámbito de aplicación de la norma. Ilustrando el problema, si se considera que una medida de protección puede ser una bolsa plástica que cubre una revista puesta en un estante de un supermercado, removerla sería, en principio, un acto de elusión de una medida tecnológica de protección y por tanto contrario a derecho. La pregunta sería si una bolsa plástica puede considerarse como una medida tecnológica.

En opinión de quien escribe, la medida sólo se puede concretar en cualquier objeto de carácter electrónico, digital o similar, que cumpla una función de control sobre la obra y las acciones humanas que interactúan con ella.

Para llegar a esa conclusión he tomado en consideración varios datos. Primero, el carácter "tecnológico" de la medida; segundo, las definiciones de "medida" proporcionadas por las legislaciones que han desarrollado la materia; tercero, los datos legislativos sobre las formas de elusión de la medida; cuarto, una razón histórica; y quinto, una consideración sobre los efectos de la regulación de esta materia.

Respecto de lo primero, entiendo por *tecnología* "[…] [un] término general que se aplica al proceso a través del cual los seres humanos diseñan herramientas y máquinas para incrementar su control y su comprensión del entorno material […]"[18]. Debo señalar que para el tema del presente escrito es la primera parte de la definición la que más me interesa: la tecnología como el proceso mediante el cual los seres humanos diseñan herramientas o máquinas para incrementar su control sobre el entorno material.

Si se acepta la noción de tecnología expuesta, también se debe aceptar que el adjetivo de "tecnológico" debe atribuírsele a toda máquina o herramienta diseñada por el ser humano para incrementar su control sobre el entorno material. En consecuencia, la medida "tecnológica" se restringe a una máquina o herramienta (en sentido amplio) que controle la obra en su relación con ciertas conductas humanas que se dan en el entorno que la rodea.

El segundo posible elemento del cual me puedo valer para determinar el objeto en que se concreta la medida se encuentra en la forma como ella ha sido definida en las legislaciones que han desarrollado el tema. En efecto, se le ha conceptuado como un producto, dispositivo y componente[19].

18. Microsoft® Encarta® 2007. ©1993-2006 Microsoft Corporation. Reservados todos los derechos.

19. 296ZE (legislación inglesa): "(1) In sections 296ZA to 296ZE, "technological measures" are any technology, device or component […]". En la normatividad australiana se dispone: "*Techonological protection measure* means a device or product, or a component incorporated into a process […]".

Entiendo por *producto*[20] algo que ha sido hecho o creado por una persona, máquina o proceso natural; por *dispositivo*[21], una herramienta o máquina diseñada para desarrollar una función o tarea particular[22]; por *componente*[23], una parte de un complejo mecánico o eléctrico.

Creo que las expresiones con las que se pretende definir el objeto en que se concreta la medida no son taxativas, sino que son enunciados que el legislador ha dispuesto para orientar al aplicador del derecho sobre qué puede ser la medida, resaltando cada una un aspecto particular: el origen y la comercialidad (producto); la funcionalidad (dispositivo); el carácter mecánico o electrónico (componente).

En mi opinión, aparte de los caracteres que el legislador quiso resaltar, las citadas expresiones no dicen mucho sobre en qué objeto se concreta una medida tecnológica jurídicamente tutelable. Creo que, hasta acá, lo único que se puede tener claro es que el objeto en que se concretará la medida debe tener un función de control en los términos que ya he señalado. Según lo dicho, parecería que la bolsa con que se cubre una revista en el estante de un supermercado es una medida tecnológica de protección, pues es un objeto que cumple una función de control sobre la revista en relación con las acciones de quienes concurren al supermercado.

Un cuarto posible elemento que puede servir de orientación es el momento histórico en que surge la normativa sobre estas medidas. En efecto, como tales, las medidas tecnológicas de protección alcanzaron una disciplina normativa en 1996 con el WIPO Copyright Treaty. El hecho de que la época coincida con un desarrollo importante de la informática y de las otras tecnologías relacionadas me hace pensar que quienes propusieron una normativa sobre el tema tuvieron este tipo de tecnología en la mente.

Un quinto elemento es el de los efectos negativos de una legislación sobre la materia interpretada de manera amplia. En efecto, me siento inclinado a interpretar de manera restringida el objeto sobre el cual puede recaer la medida tecnológica, por los potenciales efectos negativos que puede tener una legislación en esta materia sobre el sector informático, la economía digital, el libre acceso al conocimiento[24].

20. "Something that is made or created by a person, machine or natural process, specially something that is offered for sale" Microsoft® Encarta® 2007. ©1993-2006 Microsoft Corporation. Reservados todos los derechos.

21. Aclaro que el término usado en las legislaciones consultadas es "*device*", que refiero en español mediante la palabra "dispositivo". Microsoft® Encarta® 2007. ©1993-2006 Microsoft Corporation. Reservados todos los derechos.

22. "A tool or machine designed to perform a particular task or function", en Microsoft® Encarta® 2007. ©1993-2006 Microsoft Corporation. Reservados todos los derechos.

23. "A part of a mechanical or electrical complex" en [www.thefreedictionary.com], o "electric part: a device such a resistor or transistor that is part of an electronic circuit", en Microsoft® Encarta® 2007. ©1993-2006 Microsoft Corporation. Reservados todos los derechos.

24. Para más sobre estos temas, ver SAMUELSON. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", cit.

En conclusión, para definir el objeto en que puede consistir una medida tecnológica debe tenerse en cuenta principalmente el carácter tecnológico (es decir, la aptitud de control), el contexto histórico en que nació la normativa sobre la materia y los potenciales efectos negativos que se pueden derivar de una legislación sobre las medidas tecnológicas y la consecuente necesidad de interpretarla de manera restrictiva. Sumados los tres elementos, medida tecnológica sería todo objeto (producto, dispositivo, componente…) de carácter electrónico, digital o similar que por su carácter tecnológico tiene la aptitud de controlar la obra y las acciones humanas que actúan sobre ella.

2. La medida deber ser aplicada a un bien inmaterial sujeto al copyright

La medida definida en los términos indicados debe ser aplicada sobre un bien protegido por el *copyright*. Lo anterior de entrada descarta su aplicación sobre bienes que no alcanzan a ser protegidos por el *copyright*[25], que se encuentran en el dominio público o protegidos por otras ramas de la propiedad intelectual.

Al respecto vale la pena hacer la siguiente precisión: Tal como lo comenta Ricardo Antequera Parilli (*Consecuencias sustantivas de la adhesión al Convenio de Berna. Las obras protegidas*, documento ompi/da/hav/98/3), a la luz del Convenio de Berna las "obras de arte aplicado"[26] podrían ser protegidas por un ordenamiento mediante derecho de autor (o *copyright*, si el país es de esa tradición) y a la misma vez, por vía de propiedad industrial, como diseños o modelos industriales: "[…] Las anteriores consideraciones revelan la posibilidad de que una obra de arte aplicado pueda considerarse, a su vez, un diseño industrial, y que sea susceptible de protegerse, bien en el marco de la propiedad industrial (como diseño) o en el del derecho de autor (como arte aplicado), o en el ámbito de ambas disciplinas". Más adelante, refiriéndose al caso francés, comenta: "[…] la posición francesa –que cada vez gana mayores adeptos en la doctrina y en las legislaciones de tradición latina–, no establece ninguna distinción excluyente entre el arte aplicado y el diseño industrial, y por tanto admite la posibilidad de protección acumulada por ambos

25. En *Lexmark International, Inc v Static Control Components*, la Corte del Sexto Circuito de Apelaciones consideró que la secuencia de autenticación sha-1 aplicada por Lexmark no era una medida tecnológica de protección respecto del Toner Loading Program. Entre otras razones, la Corte señaló que –en caso de que se hubiese establecido que efectivamente controlaba el acceso– sha-1 no había sido aplicada sobre una obra protegida por el *copyright*, pues el Toner Loading Program, a pesar de ser un *software* no era protegible. La explicación consiste en que factores externos (requerimientos de eficiencia, funcionalidad, compatibilidad…) restringían su posibilidad de expresión hasta el punto de que esa misma idea-función no podía ser expresada de otro modo. Y, dado que el *copyright* no protege ideas, métodos o funciones, tal forma de expresión no podía ser protegida (doctrinas del *merger* y del *scénes a fair*). Para un análisis detallado de este punto, remitirse al texto de la sentencia.

26. Antequera, citando la "Guía del Convenio de Berna", define las obras de arte aplicado como *las contribuciones de orden artístico que efectúan autores de diseños o modelos en bisutería, joyería, orfebrería, fabricación de muebles, de papeles pintados, de ornamentos, de prendas de vestir, etc*.

sistemas, siempre que, por su puesto, el bien sobre el cual se reclama la tutela reúna los requisitos existenciales establecidos en los regímenes respectivos".

En conclusión, un bien intangible tutelado como diseño o modelo industrial podría ser a su vez (si el ordenamiento lo prevé) protegido mediante el *copyright* (o mediante derecho de autor) y por tanto a la persona que eluda una medida tecnológica aplicada sobre tal bien le serían atribuibles las consecuencias civiles y penales que prevé la legislación sobre la materia.

Como comentario adicional sobre este punto, vale agregar que la jurisprudencia ha señalado que la aplicación de la medida tecnológica, en contra de lo que se podría deducir del tenor literal de las normas, no debe ser necesariamente sobre la obra en sí, pudiendo estar en otro objeto (*v. gr.*, un *hardware*), siempre y cuando cumpla con los otros elementos de su definición normativa[27].

3. Especial finalidad a la que debe estar afectada la medida tecnológica aplicada sobre la obra: la prevención o inhibición de infracción al copyright o el control de acceso a la obra

Tal como se verá a continuación, la especial finalidad de protección de los derechos del titular de la obra o el control de acceso es un elemento central de las medidas tecnológicas. Cualquier mecanismo tecnológico que sirva a otras finalidades distintas no podrá considerarse como medida tecnológica en estricto sentido jurídico.

Este elemento es precisamente el que en mayor medida diferencia a la medida tecnológica de la *digital rights management* (DRM). La DRM posee la función de identificar la obra y su titular (o autor) e informar sobre los términos y condiciones bajo los cuales puede ser explotada. Con ello se pretende alcanzar dos objetivos básicos: por un lado, poner a disposición del público información confiable sobre la obra y la forma en que puede ser explotada; por otro lado, crear incentivos a los autores y titulares para que pongan a disposición sus obras en forma digital. En términos generales, la DRM está jurídicamente protegida mediante la sanción a quien altere o remueva la información vinculada a la obra[28].

Señalado lo anterior, se procede a comentar las finalidades que ha de perseguir una medida tecnológica para que jurídicamente se le pueda considerar como tal.

27. *Sony v Gaynor David Ball and other*, High Court of Justice, Chancery division, Mr. Justice Laddie, 19 July 2004 (num. 42-43).

28. "[…] The 'digital agenda' sought to further the digital dissemination or works not only by protecting digital formats against circumvention of accompanying technological measures, but also to secure the information identifying the work and the terms and conditions of its exploitations. For those who seek to make lawful use of *copyright*ed works in the digital environment, easy acquisition of accurate and reliable information about the availability and price of right enhances the likehood that new formats or new versions will be disseminated to the public. The protection of rights management information against falsification thus advances important goals whose achievement will further both the interest of authors and of the broader public in the digital communication of works of authorship […]": Sam Ricketson y Jane C. Ginsburg. *International Copyright and Neighboring Rights*, 2.ª ed., vol. II, Oxford University Press, 2006, p. 983.

a. La prevención o inhibición de infracciones al *copyright*

Para que una medida tecnológica reciba tutela jurídica se requiere que esté afectada a la especial finalidad de prevenir o inhibir la infracción del *copyright* de la obra sobre la cual ha sido aplicada.

La primera dificultad de interpretación es determinar si los derechos por proteger son exclusivamente los patrimoniales o si también ha de incluirse los morales. En el plano internacional, el lenguaje del artículo 11 del convenio es lo suficientemente abierto como para entender que los derechos que se han de proteger pueden ser tanto los patrimoniales como los morales[29]. En el plano nacional la situación es diferente. La reticencia de los países de sistemas de *copyright* respecto de los derechos morales[30] también se manifiesta en el campo de las medidas tecnológicas. En el caso específico de Estados Unidos, de la interpretación gramatical de la norma surge la posibilidad de que las medidas tecnológicas sean usadas para proteger derechos morales[31]. Sin embargo, en la práctica parece bastante difícil ya que los supuestos donde pueden surgir derechos morales son bastante restringidos y difíciles de encontrar en el mundo digital (*v. gr.*, esculturas, obras de único ejemplar). Por lo tanto, considero que aunque es teóricamente posible –al menos en el caso de Estados Unidos– la aplicación de medidas tecnológicas para la protección de derechos morales, en la práctica es poco viable.

La segunda dificultad se presenta en relación con el significado y alcance de la "prevención" o "inhibición" (u otras fórmulas legislativas semejantes). Un buen ejemplo de este problema es el caso de los *mod chips* resuelto por la Suprema Corte australiana en 2005. Los hechos relevantes de este caso son los siguientes: Sony distribuye en Australia su consola de videojuegos PlayStation. También produce y vende videojuegos en CD-ROM para uso en dicha consolas.

"El CD-ROM que contiene un juego de computadora, también contiene un 'código de acceso' (*access code*), el cual consiste en un cadena de sectores encripta-

29. Ibíd., pp. 973-974.

30. "The U.S *copyright* system has had an uneasy relationship with moral rights since the United States joined the Berne Convention [...] in 1989. [...] Although U.S adherence to the Berne Convention prompted many changes to the U.S *copyright* law, Congress initially declined to establish a full-fledged moral rights regime. The United States instead took the position that various common law causes of action, including the right of privacy, the right of publicity, defamation and unfair competition, provided rights equivalent to the moral rights required in Article 6 bis [...] Doubts nevertheless persisted over whether United States had fully met it Bern Convention obligations. Congress responded by enacting the Visual Art Act of 1990 ("VARA"). Principally codified at § 106A, VARA provided rights of attribution and integrity for certain works of visual art.": SCHECHTER y THOMAS (p. 139).

31. La §1201 (b) (1) habla de la elusión de medidas tecnológicas que "*protects a right of a copyright owner under this title*". El título al que se refiere es el 17. Las secciones 106 y 106A están contenidas en dicho título. La primera reconoce los derechos patrimoniales del autor y la segunda (introducida por el 1990 por el VARA) reconoce en los supuestos restrictivos que hemos comentado los derechos morales de atribución e integridad. Por lo anterior es mi opinión que –al menos en el plano jurídico– una medida tecnológica pueda tener por objetivo válido la protección de derechos morales.

dos de datos. Distinto de lo que ocurre con el juego de computadora, el código de acceso no puede ser accedido o reproducido por un dispositivo convencional de copiado de CD-ROM (*v. gr.*, un quemador de CD). Después de que un CD-ROM es insertado en la consola, y antes de que el videojuego pueda ser ejecutado, un *boot rom chip* en la consola debe leer la cadena de datos encriptados. Si una copia infractora del juego de computadora es insertada en la consola, el código de acceso no será encontrado en el CD-ROM y de esta manera el *software* del juego no será cargado"[32].

El demandado instalaba en las consolas de PlayStation un chip denominado *mod chip* que permitía a la consola ejecutar copias de juegos de PlayStation que carecen del código de acceso que las consolas australianas reconocen, entre ellas, copias hechas sin permiso o licencia de Sony.

La defensa replicó argumentando que el demandado no era responsable de la elusión de los dispositivos implantados por Sony (*el boot rom* y el *access code*) porque dichos medios no cumplen la función de prevenir e inhibir la infracción del *copyright*, y que por ende, lo eludido no era una medida tecnológica según la definición normativa. La respuesta a tal argumento de las distintas instancias no fue unánime.

El juez federal SACKVILLE (quien fungió como primera instancia) sostuvo que "el *boot rom* o el código de acceso no fueron 'diseñados […] para prevenir o inhibir la infracción del *copyright*' en el juego de computadora". Agregó que fueron concebidos, entre otras cosas, sólo para "disuadir o […] desanimar la infracción del *copyright* mediante la ilegítima elaboración, importación o distribución de copias de juegos de PlayStation"[33]. Y "la disuasión o el desánimo es insuficiente [en los términos de las normas citadas] para 'inhibir la infracción del *copyright*' porque la definición […] dice que si no fuera por la operación del dispositivo o producto, no habría barrera tecnológica o quizá técnica para obtener acceso a la obra protegida, o hacer copias de la obra después de que el acceso ha sido obtenido […]"[34].

Agregó también que la definición normativa no se ocupaba de "dispositivos o productos que no prevengan o disminuyan, *mediante su operación*, actos específicos que infrinjan o faciliten la infracción del *copyright* en una obra, sino que tengan sólo un efecto general de disuasión o desánimo en quienes pudiesen estar considerando infringir el *copyright* en una clase de obras, por ejemplo mediante la elaboración de copias ilegítimas de un CD-ROM" (énfasis agregado)[35].

32. *Stevens v Kabushiki Kaisha Sony Computer Entertainment* [2005] HCA 85 (6 October 2005), num. 110 (traducción libre).

33. "Justice Sackville held, however, that the Boot ROM and/or the access code were not "designed… to prevent to or inhibit the infringement of *copyright*" in the computer game. His Honour held that they were intended, *inter alia,* only to "deter or otherwise discourage *copyright* infringement by the unlawful making, importation and distribution of copies of PlayStation games": ibíd., num. 117.

34. Ídem.

35. Ídem. Para mayor claridad debo señalar que Sony había argumentado que el significado de "prevenir" e "inhibir" en la norma se refieren "disuadir o desanimar"

Creo que lo anterior puede plantearse en los siguientes términos: para el juez de primera instancia, la medida tecnológica de protección, para que sea considerada como tal a la luz de las normas relevantes, debe prevenir o inhibir "física" y efectivamente, mediante su operación, la realización de actos que puedan infringir el *copyright*. Si el dispositivo simplemente disuade (como efecto general) a las personas de infringir el *copyright*, no se le puede considerar como una medida tecnológica de protección.

En el caso concreto, el *boot rom* incorporado en la consola del PlayStation o el código de acceso insertado en los CD-ROM sólo impedían *acceder* al juego cuando el CD no tenía el código de acceso por ser una copia ilegítima; mas *no impedían que insertado un juego en la consola se realizara alguno de los actos contrarios al* copyright *del titular*, *v. gr*., copiar el juego[36].

Por el contrario, la operación de dichos mecanismos suponía que antes de insertar el juego en la consola se hubiese copiado el CD, mas no prevenían o inhibían que insertado el juego se realizara la copia. En otras palabras, los mecanismos suponían la infracción al *copyright* –copiar el CD–, mas no la impedían –porque ya se había realizado.

De esta manera, la función efectiva de dichos mecanismos queda reducida a simplemente controlar el acceso a la obra, función no tutelada por la norma australiana con la que se resolvió el caso.

De tal suerte, el juez no consideró que lo eludido fuera una medida tecnológica de protección, y por ende se desestimó la demanda de Sony.

La decisión de la Corte Federal en pleno. Sony apeló y reiteró su argumento relativo al significado de la norma. Actuando como juez de segunda instancia, la Corte Federal en pleno revocó la decisión del juez Sackville. Sostuvo lo siguiente en relación con la definición de medida tecnológica de protección: "No tiene ninguna relevancia que la inhibición sea indirecta y opere antes que el hipotético intento de acceso y la hipotética operación del dispositivo de evasión".

También agregó que algunos documentos muestran que "las palabras abiertas [de las normas relevantes] unidas con el parágrafo (a) de la definición de 'medidas tecnológicas de protección' fueron pensadas para abrazar tal inhibición, en el sentido de '*deterrence or discouragement of infringment*', lo cual resulta de una negación de acceso a […] un programa copiado en infracción del *copyright*"[37].

la infracción; efecto que, según Sony, se logra en los jugadores de PlayStation porque al saber que la consola no lee CD quemados, se abstendrían de copiarlos (es decir de infringir el copyright).

36. En este punto se debe tener en cuenta que tanto el juez Sackville como la Corte Suprema no consideraron como una reproducción contraria al *copyright* del autor la que ocurre en la memoria ram.

37. "The extrinsic materials […] show an intention that the opening words coupled with para (a) of the definition of 'technological protection measure' were intended to embrace that inhibition, in the sense of deterrence or discouragement of infringement, which results from a denial of access to, and therefore prevention of use of, a program copied in infringement of copyright". Palabras de Lindgren, juez de la Corte Federal, citadas en la sentencia.

Como resultado de lo anterior, la Corte Federal en pleno prohibió a Mr. STEVENS vender los *mod chips* para uso en las consolas PlayStation y los CD-ROM de Sony.

Corte Suprema australiana. Mr. STEVENS nunca discutió que no hubiera vendido dispositivos de elusión. En realidad lo que estuvo en cuestión es si el *boot rom chip* y el *access code* se acoplan al ámbito y a la extensión de la definición de medida tecnológica de protección de la s. 10 (1). La apelación de Mr. STEVENS ante la Corte Suprema australiana giró, precisamente, sobre el argumento de que la Corte Federal en pleno erró al considerar que dichos elementos se ajustaban a la definición.

Para la Corte, "la tarea crucial para el resultado de esta apelación es una de interpretación de las normas estatutarias, particularmente la interpretación de las expresiones definidas 'medidas de protección tecnológica' como aparece en el conjunto de la Div. 2A"[38].

Para el efecto, la corporación trae a colación las reglas aceptadas por los jueces ingleses para interpretación de las normas; sin embargo, es en la norma australiana Acts Interpretation Act 1901 en donde se detiene. Según la s. 15AA de dicho cuerpo legislativo, en la interpretación de una norma, aquella que promueva el propósito o el objeto que subyace debe ser preferida. La s. 15AB dispone que en la realización de la anterior interpretación, el juez puede valerse de una amplia gama de antecedentes legislativos.

En el presente caso la interpretación que atiende al propósito de la ley es inaplicable porque la s. 3 del Ammendment Act (la cual contiene una declaración de objetivos) se refiere al '*online*' *environment of the Internet*, lo cual no se compagina con el amplio ámbito de operación de la Div. 2A, tal como los hechos del presente caso lo demuestran (los cuales no se refieren al entorno *online*). Tampoco documentos relacionados con el proceso legislativo dan luz sobre cómo ocurrió que la propuesta de enmienda haya tomado la forma que tiene la norma. Lo que sugieren es que "el propósito legislativo fue expresar un compromiso inarticulado (o al menos no públicamente abierto)"[39].

Las anteriores razones llevan a la Corte a tomar la aproximación interpretativa de SACKVILLE, quien enfatizó en la necesidad de atender al texto de la norma y la estructura. Según la Corte (haciendo suyas las palabras del nombrado juez), el punto central de la definición de medida tecnológica está en que es "un dispositivo tecnológico o producto que es diseñado para producir un resultado específico (prevenir o inhibir la infracción del *copyright* en una obra) a través de particulares medios. Cada uno de los medios especificados envuelve un proceso o mecanismo

38. *Stevens v*..., cit., num. 30.

39. Ibíd., num. 32. "Nor do the extrinsic material give any clear indication of how it came to be that the Bill for the Amendment Act took the final form that it did. Indeed, the very range of the extrinsic materials, with shifting and contradictory positions taken by a range of interest holders in the legislative outcome, suggest that the legislative purpose was to express an inarticulate (or al least not publicly disclosed) compromise".

tecnológico. El medio identificado en par (a) es un código de acceso o proceso que debe ser usado para obtener acceso a la obra. El medio identificado en par (b) es un 'mecanismo de control de copiado' ". Agregó la Corte que frente al *access code*, que implica poder negar el acceso a una obra protegida por el *copyright*, el *copy control mechanism* envuelve un mecanismo que controla el grado [*extent*] y la efectividad del copiado de una obra que de otra forma podría hacerse libremente por alguien con acceso al material protegido por el *copyright*.

La conclusión es que para la Corte Suprema de Justicia australiana "una medida tecnológica de protección, como está definida, debe ser un dispositivo o producto que utilice medios tecnológicos para negar a una persona acceso a una obra sujeta al *copyright* […] o que limite la capacidad de un persona de hacer copias de una obra […] a la cual se ha obtenido acceso, y en consecuencia físicamente prevenga o inhiba a la persona de realizar actos que, si llevados acabo, infringirían o podrían infringir el *copyright* en una obra […]"[40].

Esta conclusión es contraria al entendimiento argumentado por Sony, acogido por la Corte Federal en pleno, y con fundamento en el cual Mr. Stevens había sido condenado; para esta interpretación (reitero) no es necesario que el dispositivo físicamente prevenga o inhiba a una persona de realizar actos que, si llevados a cabo, podrían infringir el *copyright*; "prevenir" e "inhibir" para esta interpretación hacen relación a que el dispositivo "tenga un efecto general disuasivo o de desánimo sobre aquellos que pueden estar considerando infringir el *copyright* en un grupo de obras, por ejemplo hacer copias de un cd-rom"[41]. Sin embargo, tal como se acaba de explicar, a juicio de la Corte Suprema dicho entendimiento no es acertado[42].

40. Ibíd., num. 38: "Sackville J concluded that: 'a technological protection measure', as defined, must be a device or product which utilizes technological means to deny a person access to a *copyright* work [or other subject-matter], or which limits a person's capacity to make copies of a work [or other subject-matter] to which access has been gained, *and thereby physically prevents or inhibits* the person from undertaking acts, which, if carried out, would or might infringe *copyright* in the work [or other subject-matter]" (cursivas agregadas).

41. Ibíd., num. 32.

42. En un muy reciente caso inglés (30 de junio de 2008), con casi idénticos hechos al comentado, la "Supreme Court of Judicature - Court of Appeal (criminal division)" apropió de forma expresa el entendimiento dado por la corte australiana al elemento en estudio. En el caso inglés la fiscalía en ningún momento planteó que la inserción de un videojuego en una consola implicara un acto de reproducción transitorio del material protegido por *copyright* en la memoria ram (vale aclarar, acto incluido expresamente dentro de las potestades del titular del *copyright* según las normas inglesas sobre la materia, s. 17) y, por lo tanto, tampoco planteó ante el jurado que la puesta en ejecución de un juego pirata en una consola y su reproducción en la memoria ram fuesen una infracción al *copyright*, para cuya prevención o inhibición se utilizaba las medias tecnológicas aplicadas por Sony, Microsoft, Nintendo y otras compañías dedicadas al negocio de los videojuegos. En cambio, el órgano acusador aseveró que el requisito de la prevención o inhibición de la infracción al *copyright* se satisfacía en cuanto por medio de esas medidas se desestimulaba la creación de mercados de copias piratas, porque las personas no tenían ningún estímulo para copiar ilícitamente un videojuego que –por la aplicación de las medidas– no sería leído por las consolas respectivas. La corte inglesa desestimó tal interpretación. Señaló: "[…] His point [el de la fiscalía] before us, and the point run at trial, was essentially this: that by selling modchips and modified consoles, Mr Higgs

Por lo anterior, la Corte Suprema revocó la decisión de la Corte Federal en pleno y ratificó la del juez de primera instancia.

b. El control de acceso a la obra

El simple control de acceso a la obra, no orientado a la prevención o inhibición de la infracción al *copyright* sobre la obra, también puede ser una finalidad perseguida por la medida tecnológica de protección tutelada jurídicamente.

Uno de los elementos que distinguen el sistema de *copyright* del sistema de derecho de autor es que en él las potestades que se le reconocen al titular de la obra son señaladas expresamente por la ley[43]. Esto implica que los actos que no estén comprendidos dentro las atribuciones señaladas en la ley pueden ser llevados a cabo sin autorización del titular y, por tanto, su libre realización no constituye una violación al *copyright*.

Señalado lo anterior, queda claro que en el sistema de *copyright* una medida tecnológica que controle, *v. gr.*, el mero acceso a la obra (o cualquier otro uso o explotación que se piense y que no esté comprendido dentro de las potestades exclusivas y excluyentes otorgadas por ley al titular de la obra) no sería tutelada jurídicamente –en principio– por no cumplir el fin de prevenir o inhibir directamente y por su operación la infracción al *copyright*.

Para solucionar esta situación y en vista de la rigidez interpretativa de las cortes respecto del significado de "*prevenir o inhibir la infracción al copyright*" y de la importancia económica de ciertos usos que pueden generar dudas en cuanto a si se

was in effect encouraging and exploiting a market for pirate games. No one would make or sell them unless they could be played. Mr Higgs was enabling that, so creating an incentive for the pirate market.- 13. That, Mr MacDonald submitted, was enough to satisfy the definition of an ETM. The measures concerned must be 'designed... to protect a *copyright* work' (s.296ZF [1]). Protection of a *copyright* work means the prevention or restriction of acts 'that are not authorized by the *copyright* owner of that mark and are restricted by *copyright*' (in short infringement). So the measures concerned will have the practical effect of preventing or restricting infringement. That, he submitted, is enough to fall within the definition.- 14. If he were right, then the Judge was correct to reject the appellant's submission at the end of the prosecution case that there was no case to answer and the convictions should stand. But we do not think that is the correct construction of the provision. We say that essentially for the same reasons as the High Court of Australia gave in Stevens v Sony [2005] HCA 58, 21 ALR 447 [...] In the end, therefore, one comes back to the UK Act. Is it enough if the technological measure is a discouragement or general commercial hindrance to *copyright* infringement or must it be a measure which physically prevents it? To our minds the position is clear – it is the latter. Neither the Directive nor the Act would have been drafted in the way that they are if such a general form of hindrance was enough.": *Neil Stanley Higgs v The Queen* [2008], EWCA Crim. 1324.

43. "[...] La descripción de los actos que componen el derecho patrimonial del autor no significa en modo alguno que la forma en que una obra puede ser explotada se limite a tales conductas. Por el contrario, la explotación de una obra admite diversas posibilidades, todas las cuales son válidas, pues en el sistema latino no se aplica el principio de tipicidad legal de los derecho patrimoniales, a diferencia de lo que ocurre en el *copyright*": SOFÍA RODRÍGUEZ MORENO. *La era digital y las excepciones y limitaciones al derecho de autor*, Bogotá, Universidad Externado de Colombia, 2004, p. 39.

enmarcan o no dentro una de las potestades del titular del *copyright*[44], la legislación anglosajona desde un inicio (*v. gr.*, Digital Milenium Copyright Act [DMCA] en Estados Unidos) o mediante reformas (*v. gr.*, el Ammendement Act australiano de 2006) ha incluido el mero control de acceso a la obra como una finalidad que puede perseguir una medida tecnológica tutelada jurídicamente.

De esta manera, en algunas legislaciones anglosajonas coexisten dos regulaciones sobre medidas tecnológicas de protección con ámbitos de prohibición de conductas de elusión diferentes: unas que prohíben la realización de conductas efectiva o potencialmente elusivas de medidas tecnológicas que directamente previenen o inhiben la infracción al *copyright* de las obras sobre las cuales se aplica; y otras que prohíben la realización de conductas efectiva o potencialmente elusivas de medidas tecnológicas que controlan el acceso a la obra (acto no comprendido dentro del *copyright*), sea que el control de acceso se realice sin ninguna relación con el ejercicio del *copyright* sobre la obra (*v. gr.*, DMCA) o que se exija alguna conexión (reforma australiana de 2006).

En este sentido, se debe recordar que en el caso de los *mod chips* al no aceptarse la prevención o la inhibición en el sentido de "desalentar de forma general la realización de conductas que infrinjan el *copyright*", lo que en la práctica terminaba controlando esa medida tecnológica no era la realización de un acto comprendido en los derechos exclusivos del titular de la obra[45], sino el simple *acceso* al juego contenido en el CD o DVD. Fue por esto, debe resaltarse, por lo que la corte australiana consideró que la medida aplicada por Sony no quedaba comprendida dentro de la definición normativa y, por tanto, no era tutelada por el derecho.

Tal como se dijo atrás, las legislaciones anglosajonas han reconocido tutela a dos modalidades de medidas tecnológicas que simplemente controlan el acceso a una obra: un control de acceso puro y otro que debe hacerse en *conexión* con el ejercicio del *copyright*.

Respecto de la primera forma, la sección 1201 estadounidense señala la prohibición según la cual "ninguna persona deberá eludir una medida tecnológica que efectivamente controla el acceso a una obra protegida bajo este título"[46]. Asimismo

44. Volviendo sobre el caso de los *mod chips* mencionado, y partiendo de la premisa de que el ordenamiento sólo tutelará medidas que tengan por fin prevenir o inhibir la infracción al *copyright*: si se entiende que la copia transitoria en RAM es un acto de reproducción el ordenamiento tutelaría una medida que controle el acceso al videojuego pues el acto de acceso necesariamente implicaría uno de reproducción (el cual está comprendido expresamente dentro de las facultades patrimoniales del titular del *copyright*); por el contrario, si la copia en RAM no se considera un acto de reproducción, la medida tecnológica que ejerza un control sobre el acceso a la obra no sería tutelada, pues dicho control no tendía por fin prevenir o inhibir la infracción al *copyright*. Muy seguramente para evitar tal inseguridad y para dar tutela a una forma de explotar la obra cada vez más importante, como es el acceso, las legislaciones han ampliado la finalidad que puede cumplir una medida tecnológica jurídicamente tutelada.

45. Siempre y cuando se parta –como lo hizo la corte australiana, conforme a su normatividad vigente en ese momento– de que la copia transitoria en la memoria ram no es un acto de reproducción.

46. S. 1201. Circumvention of copyright protection systems `(a) Violations regarding

prohíbe el tráfico de dispositivos destinados a la elusión de medidas tecnológicas que efectivamente controlan acceso a una obra. Aparte de que la obra debe ser protegida por el *copyright*, la norma en comento no requiere que la medida tecnológica persiga nada en particular respecto de los derechos sobre la obra.

Lexmark International, Inc v Static Control Components, Inc es un precedente judicial ilustrativo respecto de lo que debe entenderse por "controlar el acceso".

En el caso concreto, Lexmark demandó a Statics Control por venta de dispositivos que eludían –en su concepto– la medida tecnológica instalada por él en unos cartuchos respecto de los cuales se acordaba con los usuarios que sólo podían utilizarse una vez (*prebate cartridges*). La medida aplicada, conocida como SHA-I, consistía en una secuencia de autenticación que impedía a los usuarios utilizar cartuchos "prebate" no autorizados por Lexmark (esencialmente, vueltos a llenar o remanufacturados por terceras partes distintas de Lexmark). Lexmark alegó que el DMCA era aplicable porque el SHA-1 prevenía el acceso a dos programas, siendo pertinente, para lo que se está comentando, el Printer Engine Program, que se encontraba instalado en la impresora y mediante el cual se controlaban varias funciones de impresión de las impresoras (la entrada y el movimiento del papel, el movimiento del motor…).

La Corte del Sexto Circuito reversó la decisión de la corte del distrito por varias razones. En este momento interesa aquella relacionada con el alcance del concepto de "acceso" en el contexto del DMCA. La Corte manifestó que el acceso consiste en la *posibilidad de hacer uso* de la obra; pero precisó el concepto añadiendo que el uso que se ha de prevenir es el del *material expresivo* que constituye la obra y no de otros usos o funcionalidades que pueda manifestar la obra. En el caso concreto, señaló que el SHA-I no prevenía el acceso al código del Printer Engine Program (obra protegida por el *copyright*), porque él podía ser fácilmente accesible por varios medios, y en cambio sólo tenía la facultad de prevenir la *operación* ("uso") del programa (*v. gr.*, el movimiento del motor de la impresora). Concluyó que la operación de la impresora no es un uso de material expresivo y, por tanto, las medidas que controlan tal operación no son protegibles vía DMCA. Conviene señalar que la Corte distinguió este caso de aquellos otros en los que la ejecución del código resulta en material expresivo (DVD continentes de películas o videojuegos), en los cuales el control tecnológico de su acceso (usos como ver la película, jugar el videojuego…) sí resulta protegible jurídicamente[47].

circumvention of technological measures- (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

47. "[…] Lexmark counters that several cases have embraced a 'to make use of' definition of 'access' in applying the dmca. While Lexmark is partially correct, these cases (and others as well) ultimately illustrate the liability line that the statute draws and in the end explain why access to the Printer Engine Program is not covered.- In the essential setting where the dmca applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. For example, the encoded data on CDs translates into music and on dvds into motion pictures, while the program commands in software for video

Debe resaltarse cómo esta decisión crea una vinculación entre la protección de acceso ofrecida por las medidas tecnológicas y el *copyright*, vinculación que no es de origen legal pues el DMCA simplemente declara –sin más– la protección de medidas que protejan el acceso a la obra. En efecto, esta decisión crea tal vínculo al requerir que al acceso-uso a prevenir sea uno sobre el *material expresivo* y no uno relacionado con la operación o función práctica de la obra. Esta consideración jurisprudencial parece más ajustada al tratado OMPI que la regulación prevista en el DMCA.

En *términos generales*, esta decisión es la consecuencia y concreción de las brillantes consideraciones realizadas antes por la Corte de Apelaciones para el distrito federal en *Chamberlain Group, Inc. v. Skylink Techs., Inc*. No es del caso profundizar en el contenido de esta magnífica decisión por desbordar los propósitos de este escrito. Basta decir que *Chamberlain* dejó claro que en la interpretación del DMCA, en lo que respecta a medidas tecnológicas, debe tenerse en cuenta el vínculo repetido en la norma entre el *acceso* y la *protección* de los derechos conferidos por el *copyright*. De los razonamientos que parten del análisis de tal vínculo concluyó que el DMCA sólo protege aquellos controles de acceso que guarden una relación razonable con los derechos conferidos por el *copyright*[48].

Otras legislaciones, tal como se señaló, requieren que el control de acceso se realice en conexión con el ejercicio del *copyright* sobre la obra[49]. Esta solución

games or computers translate into some other visual and audio manifestation. In the cases upon which Lexmark relies, restricting 'use' of the work means restricting consumers from making use of the copyrightable expression in the work. […] The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or dvds, 'using' or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional: the Printer Engine Program 'controls a number of operations' in the Lexmark printer such as 'paper feed[,] paper movement[,] [and] motor control. […] our reasoning […] turns on the textual requirement that the challenged circumvention device must indeed circumvent something, which did not happen with the Printer Engine Program. Because Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work (the Printer Engine Program) cannot be read and copied, it cannot lay claim to having put in place a 'technological measure that effectively controls access to a work protected under [the copyright statute].' 17 u. s. c. § 1201(a)(2)(B).": Lexmark International, Inc v Static Control Components, Inc, United States Courts of Appeals – For the Sixth Circuit, October 26, 2004.

48. "[…] We conclude that 17 U. S. C. § 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords *copyright* owners. While such a rule of reason may create some uncertainty and consume some judicial resources, it is the only meaningful reading of the statute. […]": *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 2004 U. S. App. Lexis 18513, at *52 (Fed. Cir. Aug. 31, 2004).

49. Señala la normatividad australiana reformada en 2006:

"[…] *access control technological protection measure* means a device, product, technology or component (including a computer program) that:

(a) is used in Australia or a qualifying country:

(i) by, with the permission of, or on behalf of, the owner or the exclusive licensee of the copyright in a work or other subject-matter; and

(ii) *in connection with the exercise of the copyright*;

legislativa es quizá más conforme con el tenor del Tratado OMPI sobre derechos de autor de 1996[50].

Si el caso australiano de los *mod chips* al que se aludió hubiese sido resuelto bajo una normativa que tutelara una medida tecnológica cuya finalidad fuera simplemente el control de acceso a la obra (y aun bajo aquella que exige una "conexión" con el *copyright*), habría tenido un desenlace distinto. En efecto, a Sony le hubiese bastado demostrar que el *acces code* y el *boot rom* son mecanismos diseñados para controlar que ciertos juegos (copias ilegítimas o juegos de una zona distinta de la que corresponde a la de la consola) no puedan ser accedidos y, además, que la implantación de dicho mecanismo (código de acceso-chip) en la consola está en conexión con el ejercicio de los derechos que emanan del *copyright* (en caso de que la legislación lo requiera), puesto que mediante él se pretende desanimar en los usuarios la copia de los juegos y de esa forma prevenir potenciales futuras infracciones al *copyright*.

4. La medida debe ser efectiva en el control del acceso o en la prevención o inhibición de la infracción de los derechos del titular de la obra

La efectividad consiste en controlar el acceso a la obra o protegerla por medio de mecanismos tecnológicos[51]. Algunas legislaciones, atendiendo al significado común de la palabra, han agregado que a través de los medios tecnológicos la medida debe *lograr* el control o la protección pretendida.

Así las cosas, la efectividad de la medida, como requisito, se predica tanto del control de acceso como de la prevención e inhibición de infracción que otorga a la obra protegida.

Por un lado, se considera que una medida controla efectivamente el acceso cuando en "el curso ordinario de su operación requiere la aplicación de información, o un proceso o tratamiento, con el permiso del titular del *copyright*, para obtener acceso a la obra"[52].

Por otro lado, una medida protege efectivamente una obra cuando por medio de mecanismos tecnológicos (mecanismo de control de acceso, o un proceso como encriptación u otra transformación de la obra o un mecanismo de control de copia)

(b) in the normal course of its operation, controls access to the work […]" (cursivas agregadas).

50. "Las partes contratantes proporcionarán protección jurídica y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores *en relación con el ejercicio de sus derecho en virtud del presente Tratado o del Convenio de Berna*, y que respecto de sus obras restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la ley" (cursivas agregadas).

51. RICKETSON y GINSBURG (vol. II, p. 972) parecen creer que esta no es en realidad una definición de la efectividad sino una aclaración respecto de los tipos de medidas tecnológicas protegibles. Ver enseguida el desarrollo de este aspecto de la efectividad.

52. El DMCA dispone en la Section 1201: "[…] (3)`(B) a technological measure '*effectively controls access to a work*' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work".

previene, restringe o limita actos que no han sido autorizados por el titular del *copyright* y son restringidos por el *copyright*[53].

Dicho lo anterior, conviene hacer un comentario sobre el elemento de la noción, incluido por algunas legislaciones, consistente en requerir que la medida *logre* la protección o el control buscados.

El artículo 11 del Tratado OMPI de 1996 introdujo la efectividad como un componente de la medida tecnológica, pero sin especificar en qué debía consistir[54].

El DMCA interpretó la efectividad en el sentido de que la medida tecnológica " 'en el curso normal de su operación' de cualquier forma restringe el acceso o el ejercicio de algún derecho de *copyright* sobre la obra. Lo que parece ser suficiente para que el titular del *copyright* intente proteger la obra con una medida tecnológica, sin importar si, por ejemplo, pueden eludir fácilmente la medida"[55].

La Directiva de Derechos de Autor de la Unión Europea va un paso más allá del DMCA en la construcción del significado de efectividad al señalar que la medida debe "lograr este objetivo de protección"[56]. Este requisito de la directiva europea hace que la definición de efectividad "dependa fundamentalmente de *hechos empíricos*"[57]. Lo anterior ha sido mayoritariamente interpretado como una forma de *efectividad subjetiva* que se "podría establecer cuando un usuario final promedio puede eludir fácilmente la medida, ésta ya no es efectiva"[58]. Esta interpretación se

53. Dispone la normatividad inglesa en la s. 296 ZF:
"(1) In sections 296ZA to 296ZE, 'technological measures' are any technology, device or component which is designed, in the normal course of its operation, to *protect a copyright* work other than a computer program.
(2) Such measures are '*effective*' if the use of the work is controlled by the *copyright* owner through - (a)an access control or protection process such as encryption, scrambling or other transformation of the work, or (b) a copy control mechanism, which *achieves* the intended protection.
(3) In this section, the reference to - (a) *protection of a work is to the prevention or restriction of acts that are not authorized by the copyright owner* of that work and are restricted by copyright; and (b) use of a work does not extend to any use of the work that is outside the scope of the acts restricted by *copyright*."
Por su parte, la s. 1201 (b)(2)(B) dispone que "(B) a technological measure 'effectively protects a right of a *copyright* owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title".

54. RICKETSON y GINSBURG (vol. II, p. 971).

55. MIKKO VÄLIMÄKI. "Continúa el Hacking, Sentencia del 25 de mayo de 2007, Corte del Distrito de Helsinki, Finlandia" (trad. JHONNY ANTONIO PABÓN CADAVID), en *Revista del Centro Colombiano de Derecho de Autor*, n.º 12, octubre de 2007, p. 87.

56. "La Directiva de Derechos de Autor de la Unión Europea, el artículo 6.3, comienza con el mismo lenguaje que la dmca. Define que una medida tecnológica es 'efectiva' si 'en el curso normal de su operación' restringe el ejercicio de un Derecho de Autor sobre la obra. Sin embargo, la directiva luego agrega un requisito adicional: 'cuando el uso de la obra o prestación protegidas esté controlada pro los titulares de los derechos mediante la aplicación de una control de acceso o un procedimiento de protección, por ejemplo, codificación, aleatorización u otra transformación de la obra o prestación o un mecanismo de control del copiado que logre este objetivo de protección'": ibíd., p. 89.

57. Ibíd., p. 90.

58. Ídem. El mismo autor contrapone la objetividad subjetiva a la objetiva pudiéndose establecer esta última cuando "cierta medida tecnológica ya no funciona para un experto en seguridad promedio, también se volvería legalmente inefectiva".

contrapondría a una *efectividad objetiva* que implica que la medida no pueda ser eludida para que pueda ser considerada como efectiva.

Finlandia, como muchos de los países europeos[59], adoptó la decisión utilizando su lenguaje original, y según consta en documentos gubernamentales, la tendencia fue la de tomar una interpretación de efectividad subjetiva[60].

En la Corte del Distrito de Helsinki se ventiló un caso en el que un "grupo de aficionados y activistas informáticos finlandeses abrieron un sitio *web* donde publicaron información sobre cómo eludir el CSS"[61]. Los activistas "fueron procesados por haber fabricado y distribuido ilegalmente un producto para la elusión y proveer un servicio para elusión de una medida tecnológica de protección efectiva".

Dos testigos técnicos en el caso sostuvieron que "el CSS es inefectivo tanto desde la perspectiva de técnicos expertos como desde la perspectiva de consumidores promedio". La Corte acogió los testimonios y declaró: "Desde que en 1999 un *hacker* noruego logró eludir el sistema de protección CSS usado en los DVD, los usuarios finales han podido obtener con facilidad en Internet y de forma gratuita, decenas de *software* similares para la elusión. Algunos sistemas operativos traen esta clase de *software* preinstalado […] la protección del CSS ya no se puede considerar 'efectiva' según la definición de la ley"[62].

En la jurisprudencia inglesa también se encuentra una referencia sobre lo que se debe interpretar por medida tecnológica efectiva. Señaló la corte inglesa que según el contexto en que es usada la expresión "efectiva", debe entenderse como algo que está diseñado para tener un efecto y no como algo que obtenga éxito invariablemente, ya que no tendría sentido que la ley sancione la elusión de una medida que no se puede eludir[63] (efectividad en un sentido objetivo).

Como conclusión, la efectividad tiene dos facetas. La primera consiste en que se apliquen ciertos mecanismos tecnológicos (encriptación, códigos de acceso, mecanismos de control anticopia, etc.) para la prevención o inhibición de la infracción del *copyright* o para controlar el acceso a la obra. La segunda –prevista por algunas legislaciones– consiste en que la medida *logre* el cometido buscado

59. La sección 396ZF (2) de la normatividad inglesa, citada atrás, también estableció tal exigencia al disponer que los medios técnicos de los que se vale la medida "lograr la protección buscada" (…*which* achieves *the intended protection*).

60. Una *interpretación objetiva* de la efectividad es criticada y normalmente descartada ya que ella haría desaparecer toda necesidad de intervención legal: "[…] were the measure not 'effective' unless it resisted attempts to circumvent it, there would be no need for legal protection; the technology would take care of itself": RICKETSON y GINSBURG (vol. II, p. 972).

61. VÄLIMÄKI. "Continúa el Hacking…", cit., p. 90

62. Fragmento de la Sentencia del 25 de mayo de 2007, Corte del Distrito de Helsinki (Finlandia), citada por VÄLIMÄKI ("Continúa el Hacking…", cit., p. 91).

63. "[…] Neither Treaty contains a definition of "effective technological measures". One can at least see where the phrase comes from. It is an odd phrase to use in English – in its context it clearly refers to something which is intended to have an effect rather than something which is invariably successful. If it meant the latter, then there would be no need to have a law preventing circumvention. Probably something was lost in translation. Fortunately the context makes the meaning clear": *Neil Stanley Higgs v The Queen* [2008], EWCA Crim. 1324.

(prevenir o inhibir la infracción o controlar el acceso). El "logro" del cometido de control ha sido hasta ahora interpretado jurisprudencialmente en dos sentidos: cuando el usuario final promedio no puede eludir fácilmente la medida (*efectividad subjetiva* –interpretación de la corte de Helsinki) y, de una manera más laxa, cuando la medida fue diseñada para tener uno de los efectos de control buscado (corte inglesa). Una tercera interpretación de carácter objetivo ha sido descartada por ambas cortes.

5. Sujeto cualificado para aplicar la medida sobre la obra protegida por el copyright

Es interesante pensar la siguiente hipótesis: ¿qué pasa si A elude una medida de protección tecnológica aplicada por B a un *software* con cuyo titular C no tiene ningún vínculo?; o, en otras palabras, ¿cualquier persona, incluyendo alguien que no tiene ninguna relación con el titular (B respecto de C), puede aplicar una medida tecnológica de protección que sea tutelable jurídicamente?

Una respuesta afirmativa sería desacertada. Aceptar que cualquier persona puede legítimamente aplicar una medida tecnológica puede conducir a una situación contraria al fin (económico o de otra clase) que se propuso el autor o titular con su obra.

Un ejemplo: el Messenger es un *software* de distribución gratuita cuyo titular (Microsoft) se beneficia de las pautas publicitarias que se anuncian por medio de él; supóngase que Yahoo! aplica una medida tecnológica de protección de modo que sólo se pueda descargar el *software* del Messenger una vez se haya visitado la página que promociona el Yahoo Messenger. Sería contrario a los intereses del titular del *software* sostener que la medida aplicada por Yahoo! es tutelable jurídicamente, y por tanto sancionable su elusión y remoción, pues implicaría un detrimento del fin económico que el titular del *software* se ha propuesto (se obstaculiza el acceso a usuarios blanco de la publicidad, lo que lleva a que cada vez hayan menos personas interesadas en pautar en ese medio) y se beneficiaría injustificadamente a la competencia.

También podría pensarse en una situación en la que un investigador publica en Internet sus hallazgos con el ánimo de que toda la comunidad tenga acceso libre a la ciencia; supongamos que una universidad sin relación alguna con el investigado o en contra de su voluntad aplica una medida tecnológica de protección que limita el acceso a los textos a aquellas personas que tengan los códigos de acceso publicados al final de la página *web* que publicita los planes académicos ofrecidos por la universidad. Sostener que la medida tecnológica aplicada es tutelable equivaldría a contrariar el designio del autor de facilitar el acceso a la ciencia a la comunidad.

La legislación australiana de 2006 legitima en la aplicación de la medida sobre la obra sólo a los siguientes sujetos: el titular del *copyright* o a su licenciatario exclusivo, o aquellos que la apliquen con el permiso o en interés de alguno de ellos[64]. Esta

64. Subsection 10 (1) (b) (i): "[…] is used in Australia or a qualifying country by, with the permission of, or on behalf of, the owner or the exclusive licensee of the copyright in a work or other subject-matter".

salida legislativa soluciona los problemas indicados atrás. Sin embargo, en ocasiones puede resultar difícil determinar cuándo se actúa en interés o en beneficio del autor o licenciatario exclusivo (*on behal of the owner or the exclusive license of the copyright*), sobre todo cuando la medida se aplica en beneficio tanto del titular de la obra (así sea mínimo) como de quien la implanta o cuando la aplicación de la medida beneficia al titular (*v. gr.*, pecuniariamente) pero a la vez contradice el fin (interés) asignado por él a la obra[65]. La correcta aplicación de esta fórmula debe darse caso por caso.

b. consecuencias jurídicas de la elusión

La aplicación de una medida tecnológica (que cumpla los requisitos legales) sobre un obra protegida por el *copyright* crea *ex lege* un deber general negativo de abstención de realizar actos que efectiva o potencialmente eludan la medida. Puede interpretarse que este deber es una concreción legal del deber general de no causar daño a otro. La desobediencia de este deber específico de abstención de no eludir –efectiva o potencialmente– una medida tecnológica constituye un caso legalmente tipificado de responsabilidad civil[66].

Quien infrinja dicha prohibición, desarrollando actos que efectiva o potencialmente eludan la medida, debe tomar sobre sus hombros una carga reparatoria a favor del titular de la medida. La legislación australiana[67] otorga el derecho a una

65. Ricketson y Ginsburg (vol. ii, p. 973) parecen creer que la cláusula "on behalf of" se refiere a intermediarios: "[…] Such a reading would disqualify protection of devices used by intermediaries on behalf of authors, thus defeating the wct's author-protective goals".

66. Claramente lo ha dicho la Corte de Apelaciones para el Circuito Federal en *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 2004 U. S. App. Lexis 18513, at *52 (Fed. Cir. Aug. 31, 2004): "The *essence of the dmca's anti-circumvention provisions is that §§ 1201(a),(b) establish causes of action for liability. They do not establish a new property right*. The dmca's text indicates that circumvention is not infringement, 17 u. s. c. § 1201(c)(1) ('Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.'), and the statute's structure makes the point even clearer. This distinction between property and liability is critical. Whereas copyrights, like patents, are property, liability protection from unauthorized circumvention merely creates a new cause of action under which a defendant may be liable. […]" (cursiva agregada).

67. 116AQ Remedies in actions under this Subdivision

*(1) Without limiting the relief that a court may grant in an action under this Subdivision, the relief may include: (a) an injunction, subject to such terms, if any, as the court thinks fit; and (b) damages or an account of profits; and (c) if the doing of an act, which is the subject of the action, involved a circumvention device—an order that the circumvention device be destroyed or dealt with as specified in the order.

*(2) In assessing damages, the court may award such additional damages as it considers appropriate, having regard to: (a) the flagrancy of the defendant's acts that are the subject of the action; and (b) the need to deter similar acts; and (c) the conduct of the defendant after the acts or, if relevant, after the defendant was informed that the defendant had allegedly done an act that would be the subject of an action under this Subdivision; and (d) any benefit shown to have accrued to the defendant as a result of those acts; and (e) any other relevant matters.

*(3) If: (a) an action has been commenced against a person under this Subdivision; and (b) the doing of an act by the person, which is the subject of the action, involved a device; and (c) the device appears to the court to be a circumvention device; the court

compensación o reparación[68] por la elusión y los daños ocurridos. Además de lo anterior, el juez puede otorgar una suma equivalente a los beneficios percibidos por el infractor[69] y ordenar la destrucción del dispositivo de elusión, si tal es el caso. La legislación inglesa, por su lado, señala que el titular de la medida tendrá respecto de quien efectiva o potencialmente la elude el mismo derecho que el titular del *copyright* respecto de la infracción del *copyright*[70].

Debe agregarse a lo dicho que la elusión en las legislaciones consultadas también origina consecuencias penales para quien realiza la conducta. En este escrito no se abordará este punto.

c. extremos subjetivos

1. Titular del derecho a la reparación

Surge la inquietud respecto de quién se encuentra legitimado a reclamar el derecho a obtener una o varias de las medidas reparatorias por la realización de un acto elusivo señalado en la ley. Surgen al menos dos posibilidades: que la legitimación corresponda a cualquier persona o que recaiga sobre sujetos determinados.

La primera opción es viable cuando se trata de acciones que reivindican intereses públicos, pero no cuando lo que se pretende obtener es tutela de un interés privado, que es lo que usualmente se presenta en los litigios sobre medidas tecnológicas. Ninguna legislación consultada confiere una legitimación de tal carácter.

La segunda opción es más ajustada a aquellas situaciones en las que los intereses en juego son privados. Las legislaciones consultadas acogen esta opción, aunque de diversas formas.

La legislación inglesa señala expresamente los legitimados. En primer lugar, el titular de la obra o su licenciatario exclusivo. En segundo lugar, la persona que provee o distribuye las copias de la obra al público y quien las comunica a éste. En tercer lugar (en los casos en que la obra sobre la cual se aplica la medida sea un programa de computador), el titular de cualquier derecho de propiedad intelectual sobre la medida aplicada[71].

may order that the device be delivered up to the court upon such conditions as the court considers appropriate.

68. *Relief*: "*The redress, or benefit, given by a court to an individual who brings a legal action.* The relief sought in a lawsuit might, for example, be the return of property wrongfully taken by another, compensation for an injury in the form of damages, or enforcement of a contract" West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved, en [www.thefreedictionary.com].

69. *Account of profits*: "*account of pro its* A legal remedy available as an alternative to *damages in certain circumstances, especially in breach of *copyright cases. The person whose copyright has been breached sues the person who breached it for a sum of money equal to the gain made as a result of the breach", tomado de *Book*; Oxford University Press, 1996 en [www.questia.com/PM.qst?a=o&docId=48034538].

70. "S. 296 ZA: "[…] The following persons have the same rights against B *as a copyright owner has in respect of an infringement of copyright* […]".

71. Section 296. "[…] (2) The *following persons* have the same rights against A as a

El DMCA (s. 1203) contiene una fórmula amplia. Dice que toda persona que sufra un daño por elusión tiene legitimación para incoar una demanda[72]. Esto implica que no sólo el titular de la obra sobre la que se ha aplicado la medida tendrá legitimación para demandar sino otras personas, siempre que acrediten el padecimiento de un daño por la elusión. Claro, la legitimación estará siempre en primer lugar en el titular del *copyright* de la obra sobre la cual se ha aplicado la medida o en su licenciatario exclusivo.

La ampliación de la legitimación más allá del titular de la obra obedece al reconocimiento de la dinámica de varios tipos de negocios de distribución de contenidos digitalizados. En tales negocios el sujeto más afectado con la elusión no es el titular de la obra sino un tercero que tiene algún vínculo con la medida. Así mismo, en tal situación, la promoción del comercio electrónico, efectiva protección de los titulares de derechos *copyright* en el entorno digital, y la realización efectiva de los ideales de fomentar la puesta a disposición de contenidos en formato digital sólo se logran protegiendo a ese tercero. Un ilustrativo ejemplo lo constituye *RealNetworks Inc v StreamBox Inc*.

RealNetworks demandó a Streambox por violación de la prohibición de traficar dispositivos de elusión. RealNetworks es una compañía desarrolladora y distribuidora de *software* que permite a los propietarios de contenidos distribuir sus contenidos a usuarios por medio de Internet. En el caso estaban en juego tres de sus desarrollos: el RealProducer, el RealServer y el RealPlayer.

El propietario de un contenido de audio o video podía codificar sus contenidos en formato RealAudio o RealVideo, respectivamente. Una vez codificados, el propietario del contenido tiene la opción de usar el RealServer, que consiste en un *software* contenido en su computadora mediante el cual almacena y transmite los contenidos a usuarios por medio de *streaming*. El *streaming* es una forma de transmisión de música y video que, en principio, impide que los usuarios bajen una copia digital completa y perfecta al disco duro. Por el contrario, a medida que se accede al contenido se va borrando[73].

copyright owner has in respect of an infringement of copyright - (a) a person- (i) issuing to the public copies of, or (ii) communicating to the public, the computer program [u otras obras, en ciertas situaciones] to which the technical device has been applied;

(b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a); (c) the owner or exclusive licensee of any intellectual property right in the technical device applied to the computer program."

72. § 1203. Civil remedies. (a) Civil Actions. — Any person injured by a violation of section 1201 [...] may bring a civil action in an appropriate United States district court for such violation. [...]

73. "RealNetworks offers products that enable consumers to access audio and video content over the Internet through a process known as 'streaming'. When an audio or video clip is 'streamed' to a consumer, no trace of the clip is left on the consumer's computer, unless the content owner has permitted the consumer to download the file. - Streaming is to be contrasted with 'downloading', a process by which a complete copy of an audio or video clip is delivered to and stored on a consumer's computer. Once a consumer has downloaded a file, he or she can access the file at will, and can generally redistribute copies of that file to others. [...]": *RealNetworks Inc. v Streambox, Inc.*, 2000 U. S. Dist. Lexis 1889 (W. D. Wash. Jan. 18, 2000).

El sistema está diseñado para que el contenido transmitido vía *streaming* sólo pueda ser recibido por un usuario que posea RealPlayer. Ello consiste en un *control de acceso* que se logra mediante una secuencia de autenticación conocida como Secret Handshake. Sólo si se verifica la secuencia, el RealServer transmitirá vía *streaming* el contenido en cuestión. Asegurar que los archivos del RealServer sólo puedan ser transmitidos a usuarios del RealPlayer es una premisa necesaria para el funcionamiento de la segunda medida tecnológica implementada por RealNetwork: el Copy Switch. Tal medida consiste en un conjunto de datos incluidos en el archivo de audio o video mediante el cual el titular de contenido puede decidir autorizar que el *stream* sea copiado por los usuarios. De esta manera el propietario de contenidos puede prevenir la copia no autorizada. El RealPlayer fue desarrollado para obedecer lo dispuesto en el Copy Switch.

Streambox diseñó un *software* llamado Streambox VCR. Dicho *software* permite recibir el contenido transmitido mediante *streaming* del RealServer al RealPlayer. Logra tal efecto "imitando" al RealPlayer y, de esa manera, eludiendo la medida de control de acceso (Secret Handshake). Eludido el control de acceso, el Streambox VCR elude el Copy Switch, pues él, a diferencia del RealPlayer, no está diseñado para obedecer la orden de permitir o no la copia contenida en el archivo.

Tal como se puede observar, RealNetworks no es el propietario de las obras sobre las cuales se aplican las medidas tecnológicas señaladas (Secret Handshake y Copy Switch). Ello no fue óbice para que la Corte le reconociera legitimación ya que –tal como ya se dijo– la s. 1203 confiere legitimación (*standing*) a cualquier persona que acredite haber sufrido un daño (*injury*) por causa de elusión (real o potencial).

En el análisis de los hechos, la Corte precisó en qué consiste el daño sufrido por RealNetworks. Una de las tres principales fuentes de ingresos, y en cierto modo la base de todo el negocio de la empresa, es la venta del sistema de *software* necesario para el *streaming* a los propietarios de contenidos. El principal atractivo del sistema es la seguridad que ofrece a los propietarios y su versatilidad para poder realizar distintos negocios[74]. Seguridad, en cuanto pueden controlar el acceso al contenido y la copia; versatilidad, en cuanto el sistema anticopia garantiza a los propietarios de contenidos que sus páginas seguirán siendo visitadas, lo cual implica mantener o mejorar las tarifas por publicidad en la página; también el sistema permite a los propietarios ofrecer a los usuarios la posibilidad de oír o ver el contenido antes de decidir comprarlo; así mismo, el sistema permite el negocio del "pay-per-play" mediante el cual el usuario debe pagar cada vez que desee oír o ver el contenido. El tráfico del Streambox VCR reduce la capacidad de los propietarios de contenidos de controlar el acceso y la copia y, por ello, su interés por adquirir el sistema. En esa pérdida de atractivo consiste el daño sufrido por RealNetworks[75].

74. "RealNetworks' success as a company is due in significant part to the fact that it has offered *copyright* owners a successful means of [*9] protecting against unauthorized duplication and distribution of their digital works. […]": ídem.

75. "[…] RealNetworks has demonstrated that it would likely suffer irreparable harm

De no poseer legitimación RealNetworks en este caso, los objetivos de protección de los autores en el contexto digital, la promoción de comercio electrónico y la puesta en medio digital de las obras difícilmente se lograrían.

2. Sujetos pasivos de la prohibición de elusión y del derecho a la reparación

De la interpretación de la normatividad que ha desarrollado la materia y un precedente judicial parece desprenderse que puede ser sujeto pasivo toda persona que desarrolle una de las conductas descritas en la legislación, inclusive el simple usuario del dispositivo modificado para eludir la medida tecnológica.

III. INFRACCIÓN DE LA PROHIBICIÓN DE ELUSIÓN DE LA MEDIDA

La satisfacción de intereses contrapuestos a los que tutelan la regulación sobre medidas tecnológicas implica la realización de conductas antijurídicas, siempre y cuando se enmarquen en alguna de las modalidades de infracción (formas de elusión) señaladas en la ley y no hayan sido exceptuadas por el ordenamiento.

La forma como se regulan las distintas formas de infracción, o modalidades de elusión de medidas tecnológicas, es de crucial importancia: si las infracciones son reguladas en forma estrecha y restrictiva, en la práctica no se protegerán los intereses tutelados por las normas sobre medidas tecnológicas, principalmente la seguridad de los derechos de propiedad intelectual en el entorno digital; si las infracciones son reguladas de manera amplia, se pueden afectar caros intereses, especialmente los relacionados con el desarrollo del comercio electrónico y el acceso al conocimiento[76]. Vale la pena resaltar acá que la economía digital, sin ir más allá de los mundos virtuales (especialmente *Second Life*), mueve cifras impresionantes al año, además de ser una plaza prometedora para empresarios pequeños y grandes de todo el mundo[77].

if the Streambox VCR is distributed. The VCR circumvents RealNetworks' security measures, and will necessarily undermine the confidence that RealNetworks' existing and potential customers have in those measures. […]": ídem.

76. En efecto, "[…] *The Emerging Digital Economy* report continues along the path set by the Administration's early policy document, *The Framework for Global Electronic Commerce*, in seeking to foster the growth potential of the digital economy. Both documents recognize that *"[g]overnments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and -at least as important- when not to act, will be crucial to the development of electronic commerce*.": SAMUELSON. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", cit. (cursivas agregadas).

77. "In the past 24 hours 1.7m people have spent *$1.6m (£790,000)* buying land, building houses, shopping and conducting business in Second Life, a *virtual world that is rapidly developing into a sizeable real economy*. […] Big businesses including Dell, Cisco, IBM and Reuters all have a presence on Second Life but in the main the website's commercial life is dominated by virtual small business owners, some of whom are making real money. In June, 132 residents earned more than $5,000 a month on the site, up from 97 in January. A further 1,340 earned $500-$4,999 a month, up from 837 in January", en "Fancy a second life?", 15 de Julio de 2007, [http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2075004.ece].

De ahí que para la regulación de las medidas tecnológicas (y en general de todo el comercio digital) la administración Clinton haya formulado unas directrices que tienden a estructurar el modelo de regulación ideal para esta economía emergente: la regulación debe ser predecible, minimalista, consistente y simple[78].

Sin embargo, la experiencia legislativa de Estados Unidos ha dejado un sabor amargo, porque en ella, más que una valoración racional de los efectos negativos que una regulación sobre esta materia puede tener sobre la economía digital y una sujeción a los principios trazados en el Framework for Global Electronic Commerce, primaron sin mayores consideraciones los intereses de Hollywood, sobre los de otros sectores importantes en la nueva economía, como son los del sector informático[79].

En general, las legislaciones que han desarrollado este tema han creado tres modalidades de infracción: la elusión efectiva de una medida tecnológica; la realización de alguna de las conductas descritas en la ley en relación con un dispositivo de elusión; la prestación de servicios que posibilitan la elusión de la medida. La primera modalidad es aquella que a lo largo del escrito se ha denotado y se denotará como *elusión efectiva de la medida tecnológica*; la segunda y la tercera modalidades son aquellas que a lo largo del escrito se han indicado y se indicarán como *conductas que potencialmente pueden resultar en la elusión de la medida*. Brevemente se expondrá el tratamiento que se ha dado a estas modalidades.

78. "The Framework for Global Electronic Commerce:
(1)-The private sector should lead.
(2)- Governments should avoid undue restrictions on electronic commerce.
(3) -Where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.
(4)- Governments should recognize the unique qualities of the Internet.
(5)-Electronic commerce over the Internet should be facilitated on a global basis."

79. "It would oversimplify the facts -although not by much- to say that the battle in Congress over the anti-circumvention provisions of the dmca was a battle between Hollywood and Silicon Valley. Hollywood and its allies sought the strongest possible ban both on the act of circumventing a technical protection system used by copyright owners to protect their works and on technologies having circumvention-enabling uses. Silicon Valley firms and their allies opposed this broad legislation because of deleterious effects it would have on their ability to engage in lawful reverse engineering, computer security testing, and encryption research. They supported legislation to outlaw acts of circumvention engaged in for the purpose of infringing copyrights and would have supported narrowly drawn device legislation had the Congressional subcommittees principally responsible for formulating wipo treaty implementation legislation been receptive to a narrower bill. Silicon Valley and its allies warned of dire consequences if the overbroad anti-circumvention provisions Hollywood supported were adopted. Yet, by colorful use of high rhetoric and forceful lobbying, Hollywood and its allies were successful in persuading Congress to adopt the broad anti-circumvention legislation they favored, even if it is now subject to some specific exceptions that respond to some concerns raised by Silicon Valley firms and their allies in the legislative process": Samuelson. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", cit.

A. ELUSIÓN EFECTIVA DE UNA MEDIDA TECNOLÓGICA ("ANTI-CIRCUMVENTION PROVISION")

1. La conducta: elusión de la medida. Alcance

"Ninguna persona debe eludir una medida tecnológica de protección que efectivamente controla el acceso a una obra protegida bajo este título"[80]; "[…] la persona que realiza un acto que resulta en la elusión de una medida de protección tecnológica de control de acceso"[81] o "[…] una persona que realiza cualquier cosa [acto] que eluda tales medidas […]"[82] son fórmulas legislativas utilizadas para prohibir la elusión de una medida de protección.

La lectura de las fórmulas revela que la prohibición es amplia, sobre todo aquellas que enfatizan en "cualquier acto" o un "acto que resulta en la elusión". Un problema que surge al respecto es el de los alcances de la prohibición. Se considera que dicha prohibición es tan amplia que cobija aun la conducta de quien usa un dispositivo modificado que permita eludir una medida tecnológica de protección.

La jurisprudencia inglesa resolvió un caso casi idéntico al australiano comentado atrás. En este caso los demandados por Sony estaban involucrados en el diseño, la manufactura, venta e instalación de un chip electrónico llamado Messiah 2, que se instalaba en el PlayStation 2 con el propósito de hacer creer a la consola que los CD o DVD insertados contenían los códigos de acceso que poseen los CD originales. Lo anterior implicaba la posibilidad de jugar no sólo videojuegos originales vendidos en el Reino Unido, sino también la posibilidad de jugar copias ilegítimas de ellos y copias legítimas pero vendidas para un sector geográfico diferente de aquel al que pertenece el Reino Unido. Respecto de la infracción que se está estudiando, señaló la Corte: "[dado que] Mr. Ball (el demandado) ha instalado él mismo Messiah 2 y *usado la consola modificada*, así parece no haber defensa frente a este cargo" (tra-

80. Section 1201 del DMCA: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title". El DMCA solo sanciona el acto efectivo de elusión de una medida tecnológica que controla el acceso a la obra. Por el contrario, no sanciona la elusión de una medida que protege los derechos del titular de la obra. La razón es que si la elusión es para la realización de alguna de las facultades exclusivas del titular de la obra, ello terminaría en una infracción al *copyright*, y por tanto, no es necesario responsabilizar además a la persona por la elusión de la medida; bastan las consecuencias derivadas de la infracción a los derechos del titular de la obra: "To understand how it does this, you have to remember the two types of circumventions discussed above. Section 1201(b) addresses "circumvention to infringe", *and only has a trafficking provision since any infringement that results is already a violation of the copyright statutes*. Section 1201(a), on the other hand, addresses "circumvention to access," which is of importance only when there is not an infringement. […]": HOLLAAR. *A bad trade…*, cit. (p. 4) (cursivas agregadas).

81. "[…] the person *does an act that results in the circumvention of the access control technological protection measure* […]"

82. 296ZA Circumvention of technological measures (UK): "[…] (b) a person (B) *does anything which circumvents those measure* […]"

ducción libre)[83]. Parece que, según la interpretación dada a esta prohibición por la jurisprudencia, hasta los usuarios de equipos modificados (*v. gr.*, el PlayStation, reproductores de DVD, etc.) pueden ser sujetos pasivos de una demanda por infracción de las disposiciones que regulan las medidas tecnológicas de protección.

En este punto conviene plantearse qué se debe entender por la elusión de una medida. De la legislación que se ha ocupado del punto se puede deducir que la elusión de una medida tecnológica consiste en uno o varios actos –que van desde la elusión propiamente dicha, pasando el debilitamiento de la medida, hasta su remoción– sin la autorización del titular del *copyright* sobre la obra[84].

Surgen dos interrogantes respecto de la autorización. La primera es si necesariamente debe proferirla el titular del *copyright* o puede provenir de otros sujetos. La segunda versa sobre la forma en que debe proferirse la autorización.

Respecto de lo primero, parece acertado considerar que la autorización para realizar un acto que de otra manera sería considerado como elusivo de una medida tecnológica puede provenir de cualquiera de los sujetos que la legislación legitima para reclamar la indemnización, y no sólo del titular del *copyright* de la obra sobre la que se aplicó la medida. No podría ser de otra forma, pues no sería lógico que el ordenamiento legitimara a dichos sujetos para reclamar la indemnización por la elusión mas no a todos ellos para autorizarla.

83. *Sony v Gaynor David Ball and other*, High Court of Justice, Chancery division, Mr. Justice Laddie, 19 July 2004 (num. 36).

84. S. 1201 del DMCA dispone en una de sus subsecciones: "to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the *copyright* owner". Lo anterior puede ilustrarse con un ejemplo real, además de aquellos comentados ya en este escrito. La empresa CoxCom ofrecía servicios de televisión por suscripción. Dicha empresa arrendaba a sus suscriptores un equipo de decodificación ("*cable boxes*") mediante el cual los suscriptores descifraban la señal de entrada, de tal manera que se hiciera visible en las pantallas de los televisores. El equipo de decodificación no sólo recibía señal sino que también enviaba información de vuelta a CoxCom. Dicha información posibilitaba servicio de "pay-per-view", ya que transmitía a la compañía información asociada con la compra de determinada programación ofrecida mediante "pay-per-view". JON CHAFFEE y otros vendían un dispositivo llamado "digital cable filter". Tal equipo tenía varias utilidades, que iban desde mejorar la calidad de la señal recibida hasta afectar la información de retorno. En el caso en concreto, la información afectada era la de retorno de los usuarios a CoxCom respecto de la compra de programación "pay-per-view", lo cual implicaba para ésta no poder cargar a las cuentas de los usuarios la programación vista. CoxCom demandó a JON CHAFFEE por infracción a la prohibición contenida en la s. 1201 del DMCA. Una de las defensas invocadas por el demandado consistió en que sus "digital cable filter" *no eludían* medidas tecnológicas. La Corte desestimó tal argumento. Consideró: "To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner… 17 U. S. C. § 1201(3)(A). The technological measure here, as appellants acknowledge, *is CoxCom's pay-per-view delivery and billing system that scrambles pay-per-view programming unless subscribers choose to purchase and view* it. See also *CSC Holdings, Inc. v. Kelly*, 374 F. Supp. 2d 303, 303 (E. D. N. Y. 2005) (encoding and scrambling of pay-per-view and premium channels is a 'technological measure'). A digital cable filter allows subscribers to 'avoid' or 'bypass' that technological measure. […]": *CoxCom, Inc v Jon Chaffee*, United States Court of Appeals for the First Circuit, August 4, 2008 (cursivas agregadas).

Respecto de lo segundo, la jurisprudencia ha considerado que la autorización puede ser implícita. Tal fue uno de los puntos de discusión en *Chamberlain Group, Inc. v. Skylink Techs., Inc* ante la Corte para el Distrito Norte de Illinois. Ambas empresas eran productoras de sistemas para abrir y cerrar las puertas de garajes (*garage door openers* [GDO]). El sistema se compone, en esencia, de dos elementos: un transmisor portátil y un dispositivo para abrir y cerrar instalado en el garaje. Chamberlain desarrolló una línea de GDO llamada Security+. La particularidad de dicha línea consistía en que incorporaba el programa "*rolling code*" que modificaba constantemente la señal emitida por el transmisor requerida para abrir la puerta del garaje. Este cambio constante pretendía reforzar la seguridad en los GDO de Chamberlain. Skylink desarrolló el transmisor universal Model 39, que, a pesar de no utilizar la tecnología *rolling code*, tenía la aptitud de activar los GDO de línea Security+. Chamberlain demandó a Skylink –entre otras cosas– por violación de la prohibición de dispositivos. Alegó que el *rolling code* era una medida tecnológica de control de acceso a programas de computador de su propiedad, debidamente protegidos por el *copyright*, incorporados en el transmisor y en el dispositivo de abrir el garaje, que era eludida por los compradores-usuarios del transmisor Model 39, transmisor que Skylink producía y comercializaba.

Entre otras defensas, Skylink señaló que Chamberlain, a falta de restricción expresa, había autorizado implícitamente a los compradores de su sistema Security+ a utilizar otros transmisores. Tal argumento fue acepado por la Corte, razón por la cual desestimó la pretensión de Chamberlain. Al ser la operación del Model 39 implícitamente autorizada por Chamberlain, no podía considerarse una elusión en el sentido del DMCA y, por tanto, la fabricación y el tráfico de tales dispositivos tampoco podían considerarse tráfico de dispositivo de elusión. Para lo que interesa en este momento, vale recalcar que jurisprudencialmente es aceptado que la autorización sea tácita, de acuerdo con las circunstancias del caso[85].

85. En palabras de la Corte de Apelación de Estados Unidos para el Circuito Federal: "Skylink submitted several defenses […] (3) consumers use the Model 39 transmitter to activate the Security+ GDOs with Chamberlain's consent; […] Though the District Court commented on all of these arguments, it based its rulings entirely on Skylink's third argument concerning authorization and consent. […] Chamberlain noted that it never gave consumers explicit authorization to program competing universal transmitters into its rolling code openers, at least in part because it never anticipated that any competitor would crack its code. Skylink did not dispute this point, but asserted simply that in the absence of an explicit restriction, consumers must be free to infer that they have purchased the full range of rights that normally accompany consumer products including those containing copyrighted embedded software.- According to undisputed facts, a homeowner who purchases a Chamberlain GDO owns it and has a right to use it to access his or her own garage. At the time of sale, Chamberlain does not place any explicit terms or condition on use to limit the ways that a purchaser may use its products. *A homeowner who wishes to use a Model 39 must first program it into the GDO. Skylink characterizes this action as the homeowner's authorization of the Model 39 to interoperate with the GDO. In other words, according to Skylink, Chamberlain GDO consumers who purchase a Skylink transmitter have Chamberlain's implicit permission to purchase and to use any brand of transmitter that will open their GDO*. The District Court agreed that Chamberlain's unconditioned sale implied authorization. […] In short, the *District Court concluded that because Chamberlain never restricted its customers' use of competing transmit-*

2. Conocimiento de (o deber de razonablemente conocer) que con la acción se elude una medida tecnológica de protección

Este elemento consiste en el efectivo conocimiento o el deber de razonablemente conocer, según las circunstancias, que el efecto de la acción es la elusión de la medida[86]. Lo anterior excluye elusiones "accidentales", no intencionadas, de la medida.

Se debe resaltar que este elemento no aparece en la legislación de Estados Unidos. Esta ausencia es una decisión política desacertada: por un lado, elimina un elemento que crea un balance frente a la gran amplitud de la prohibición; por otro, abre paso a situaciones injustas en las que alguien debe cargar con un deber reparatorio o con una sanción penal por una elusión "accidental", es decir, no intencionada.

b. conductas respecto de un dispositivo de elusión ("anti-trafficking provisions")

1. Realización de una o varias de las conductas definidas en la ley

Se ha señalado en varias ocasiones que la medida tecnológica tutelada jurídicamente (por ajustase a los supuestos legales) crea un deber general de abstención de realizar actos que real o potencialmente la eludan. Pues bien, si la modalidad de infracción anterior tipificaba cualquier conducta que implique la elusión efectiva de una medida tecnológica, la presente modalidad de infracción tipifica conductas que sólo potencialmente pueden desembocar en la elusión de la medida. Así, manufacturar, importar[87], distribuir, vender o *lets for hire*, ofrecer o exponer para la venta o *hire*, o tener en posesión para propósitos comerciales un dispositivo de elusión da lugar a consecuencias jurídicas importantes[88].

ters with its Security+ line, those customers had implicit authorization to use Skylink's Model 39. Because of that implicit authorization, Chamberlain could not possibly meet its burden of proving that Skylink trafficked in a device designed to circumvent a technological measure to gain unauthorized access to Chamberlain's copyrighted computer programs.": *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 2004 U. S. App. Lexis 18513, at *52 (Fed. Cir. Aug. 31, 2004) (cursivas agregadas).

86. Dice la legislación australiana de la materia, enmendada en 2006: "*116AN Circumventing an access control technological protection measure*: […] (b) the person does an act that results in the circumvention of the access control technological protection measure; and (c) the person knows, or ought reasonably to know, that the act would have that result"; la legislación inglesa dice: "(b) a person (B) does anything which circumvents those measure**s** knowing, or with reasonable grounds to know, that he is pursuing that objective".

87. La legislación australiana califica estas conductas con una particular intención del agente. Así, no basta manofacturar e importar el dispositivo, sino que se debe hacer con la intención de proveerlo a otra persona: "(a) the person does any of the following acts with a device: (i) manufactures it with the *intention* of providing it to another person; (ii) imports it into Australia with the intention of providing it to another person […]".

88. Dice la norma inglesa: "*296ZD Rights and remedies in respect of devices and services designed to circumvent technological measures*: (1) This section applies where: (a) *effective*

Esta prohibición merece tres comentarios. El primero es que la decisión de tipificar como contrarias a derecho estas conductas sigue la lógica de la evitación del riesgo: importar un dispositivo de elusión no implica la elusión de una medida, pero con el castigo de aquella conducta se previene que alguien eluda una medida con el dispositivo importado.

El segundo es que esta decisión muestra una predilección legislativa por la protección de los intereses de los titulares de las medidas: se castiga la posibilidad de elusión, sin que sea necesario que esto llegue efectivamente a suceder (y sin que sea necesario, mucho menos, que se infrinja el *copyright* sobre la obra)[89].

El tercero es que esta norma permite atacar la "cadena productiva" de las medidas de elusión: a. permite que el titular del derecho consiga una posibilidad mayor de no elusión de su medida (distinto de si le limitara a demandar al usuario); b. otorga mayores garantías de satisfacción patrimonial a quien demanda (el productor, importador… probablemente tiene más dinero que el usuario del dispositivo modificado); c. evita, en la práctica, demandas a los usuarios: demandar a éstos es más engorroso y hay menos garantías de satisfacción patrimonial[90]. No por otras

technological measures have been applied to a copyright work other than a computer program; and (b) a person (C) *manufactures, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire, or has in his possession* for commercial purposes any device, product or component, or provides services which […]". Por su parte, la norma australiana prescribe: "*116AO Manufacturing etc. a circumvention* device *for a technological protection measure* (1) An owner or exclusive licensee of the copyright in a work or othersubject-matter may bring an action against a person if: (a) the person does any of the following acts with a device: (i) manufactures it with the *intention* of providing it to another person; (ii) imports it into Australia with the intention of providing it to another person; (iii) distributes it to another person; (iv) offers it to the public; (v) provides it to another person; (vi) communicates it to another person […]". El DMCA dice: "s. 1201 (a) (2): (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that […]".

89. "The wording of s 296 ZD does not define breaches of the copyright owner´s right in terms of causing or facilitating infringements of copyright. Once a protected technological measure exists, it is breach of the provision, for example, to advertise for sale any device, product, component or service which is primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of the technological measure": *Sony v Gaynor David Ball and other*, cit.

90. "Una concepción que solo tenga en cuenta el comportamiento es insuficiente por varias razones. Por regla general, el comportamiento de elusión no es público; las personas normalmente lo llevan a cabo en la intimidad de sus hogares o lugares de trabajo. Si bien los resultados de esa actividad, como un programa informático de servicio que eluda una medida de protección de ejemplares, se pueden hacer públicos, el comportamiento que lleva a forzar el sistema de protección suele ser privado. No es factible ni deseable iniciar un control sistemático de los comportamiento privados para impedir las acciones de elusión […] No obstante, si se pueden adquirir de forma legal (o recibir gratis) dispositivos o servicios que anulen estas medidas, es mucho más difícil mantener la integridad de las tecnologías de protección y éstas cumplan su objetivo. Este concepto no es nuevo. Por ejemplo, muchos países prohíben la fabricación, la venta o la distribución de 'tarjetas inteligentes' piratas o de cajas negras pirata que se usan para descifrar y obtener acceso condicionado a emisiones de televisión por cable o por satélite sin autorización y sin pagar. En consecuencia para proporcionar unos recursos efectivos contra la elusión, la ley debe proscribir los dispositivos y los servicios que se crean o se distribuyen con el objeto de eludir las tecnologías de protección": MARKS y TURNBULL. Documento OMPI…, cit., pp. 6-7. RICKETSON y GINSBURG (vol. II, p. 976) señalan que

razones algunos han sostenido esta prohibición como el corazón de la regulación antielusión de medidas tecnológicas[91].

2. Afectación de los dispositivos a una finalidad específica señalada en la ley

¿Cuál es el ámbito de la prohibición de las conductas en relación con dispositivos que puedan servir como herramientas para eludir una medida tecnológica? Un computador personal puede tener muchas funciones, una de las cuales puede, eventualmente, ser la de eludir una medida tecnológica de protección. Sin embargo, a nadie que tuviese un mínimo de consideración por el desarrollo de la tecnología y sus beneficios se le ocurriría prohibir el computador personal por tener una función no principal de elusión.

Para precisar el ámbito de la prohibición, y tratar de limitarlo a su punto apropiado[92], las conductas señaladas atrás deben versar sobre un dispositivo, producto o componente que[93]

el artículo 11 de del convenio OMPI, fundamento internacional de las prohibiciones nacionales de la elusión de medidas tecnológicas, no puede ser interpretado en el sentido de de excluir la posibilidad de considerar como ilícitos los actos preparatorios a la elusión por que tal inferencia "[…] would diminish the effectiveness of the prohibition". Como soporte de su afirmación señalan: "First, limiting the prohibition to the act of circumvention would mean that copyright owners would need to discover and prove the commission of acts that may often occur in private, at the user's home. This seems both difficult for copyright owners and undesirable to users. Second outlawing the device as well as the activity is likely to have a greater impact on the provision of circumvention devices; without the device, less circumvention is likely to occur, and it is more effective to pursue a small number of device suppliers than the large number of their customers": HOLLAAR. *A bad trade*… (p. 2).

91. "The anti-circumvention provisions of the DMCA are really about traffickers in circumvention technology, not about those using it. It keeps things off the shelves of stores so they don't seem legitimate. […]"

92. "Aunque deben aplicarse a los dispositivos y servicios unas leyes efectivas contra la elusión, no es fácil establecer los límites sobre qué dispositivos y qué servicios deberían prohibirse. Los casos extremos son relativamente sencillos. No cabe duda de que las llamadas 'cajas negras' que sirven únicamente, pro ejemplo, para descifrar señales de televisión sin autorización (es decir, eludir el control de acceso a la codificación) o para anular las medidas de protección, son dispositivos que deberían ser ilegales. En el otro extremos están los ordenadores personales comunes, que a veces usan los piratas para forzar las medidas de de protección de ejemplares que se incorporan a los soportes lógicos. A pesar de que dichos ordenadores a veces se utilizan con estos fines lícitos, no deberían prohibirse por considerarlo dispositivos de elusión porque generalmente tiene funciones y fines totalmente legítimos. El problema es trazarla línea entre los dos extremos.- La mayoría de la gente estaría de acuerdo en que la incorporación de un reloj en una 'caja negra' no debería legitimar el dispositivo sencillamente porque las funciones de cronómetro de la parte del dispositivo y donde se encontraría el reloj son legítimas. No obstante, no faltaría quien sostendría que un dispositivo que permita reproducir contenidos visuales analógicos a través de un ordenador cuya acción también tenga como resultado la eliminación de los indicadores de control de copia del contenido debería de estar permitido. En nuestra opinión, la dmca consigue equilibrio apropiado en esta materia tan delicada. Este equilibrio lo consigue, primero, estableciendo tres principios alternativos para determinar si el servicio o dispositivo debería prohibirse por su carácter elusivo […]": MARKS y TURNBULL. Documento OMPI…, cit., p. 6.

93. Dice la norma inglesa: "*296ZD Rights and remedies in respect of devices and services designed to circumvent technological measures* […] device, product or component, or provides services which - (i) are *promoted, advertised or marketed for the purpose of the*

– sea [*prompted*], publicitado o comercializado con el propósito de eludir una medida tecnológica; o

– posea sólo un limitado propósito o uso comercialmente significativo distinto de eludir; o

– sea fundamentalmente diseñado, producido o adaptado o [*performed*] con el propósito de posibilitar o facilitar la elusión de tales medidas.

Basta con que el dispositivo cumpla una de las varias condiciones para que caiga en el ámbito de la norma[94].

Las posibilidades de configuración legislativa sobre las cualificaciones que debe poseer el dispositivo son bastante amplias debido a que el convenio OMPI no dispuso nada al respecto. Sin embargo, la amplitud del legislador se debe limitar por dos criterios derivados del artículo 11 del tratado. El primero es que los estados deben proveer "efectiva y adecuada" protección a los autores que apliquen sobre sus obras medidas tecnológicas; y el segundo es que las medidas deben restringir actos no autorizados por el autor (dentro del marco de sus derechos) o por la ley. El primer criterio deslegitima de cara al tratado una cualificación del dispositivo de "cuyo único propósito o efecto sea eludir" porque, muy probablemente, cualquier demandado puede alegar y probar satisfactoriamente que el dispositivo posee otra función distinta de eludir, así sea mínima; por otro lado, frente al segundo criterio no sería legítimo que la cualificación fuese "cuyo propósito sea eludir", pues el ámbito de prohibición sería lo suficientemente amplio como para afectar usos autorizados por el autor o por la ley[95].

3. Elemento subjetivo. Conocimiento por parte del agente de que el objeto es un dispositivo de elusión de una medida tecnológica de protección[96]

Este elemento no está presente en la legislación inglesa ni en la estadounidense, sólo en la australiana. Implica que el agente de las conductas conoce, o razonable-

circumvention of, or (ii) have only a *limited commercially significant purpose* or use other than to circumvent, or (iii) are *primarily designed*, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, those measures".

El DMCA prescribe:

"1201 (a) (2) No person shall manufacture […] any technology, product […] that:

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a *technological measure that effectively controls access to a work* protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title".

La legislación australiana no cualifica los dispositivos en la forma hecha por las dos normas anteriores.

94. "These three tests are disjunctive. *Id.* A product that meets only one of the three independent bases for liability is still prohibited. […]": *RealNetworks Inc. v Streambox, Inc.*

95. Para ver más a fondo este problema: RICKETSON y GINSBURG (vol. II, pp. 977-978).

96. "*116AO Manufacturing etc. a circumvention* device *for a technological protection measure* […] (b) the person *knows, or ought reasonably to know*, that the device is a circumvention device for a technological protection measure; and […]": norma australiana citada.

mente debe conocer, que el dispositivo es de elusión de una medida tecnológica de protección.

La legislación inglesa, antes de la reforma de 2003, incluía como elemento necesario para configurar la infracción el conocimiento (o el razonable deber de conocer) de que el dispositivo sería usado para la *producción ilegítima de copias*. Este conocimiento difiere en su contenido del que enunciamos en el título de este aparte. En un caso ventilado ante la Corte Suprema inglesa, este fue un punto decisivo. En este caso (al igual que el comentado) Sony demanda a unas personas que diseñaban, importaban, distribuían, vendían e instalaban un chip llamado Messiah 2 que permitía eludir la medida tecnológica implantada por Sony en el PlayStation 2.

El abogado de la defensa alegó, entre otras cosas, que el demandado "no conoce o [no] tiene razones para creer que el Messiah 2 será usado para *hacer* '*copias infractoras*' ". La sección 27 define las copias infractoras así: "[…] (2) Un artículo es una copia infractora si su elaboración constituye una infracción del *copyright* sobre el trabajo en cuestión; (3) un artículo es también una copia infractora si: (a) ha sido o es planeado ser importada en el Reino Unido; y (b) su elaboración en el Reino Unido habría constituido una infracción del *copyright* en la obra en cuestión"[97].

El abogado sostuvo que "una copia infractora debe ser un 'artículo'. En otras palabras, debe ser demostrado que […] Mr. Ball [el demandado] conoció o tuvo razones para creer que el Messiah 2 sería usado para hacer artículos los cuales son copias infractoras". Agregó que "ninguno de estos artículos existe aquí. El Messiah 2 no es usado para hacer copias no autorizadas del CD o DVD en el cual el juego de PlayStation 2 es provisto por Sony. Tampoco es fundado que un juego de PS2, importado, pero auténtico, sea o una copia ilegítima o producida por el uso de chip Messiah 2"[98].

La parte demandante replicó que el uso de un CD o DVD sin licencia [copia pirata] o de un juego importado inevitablemente resulta en la infracción del *co-*

97. Prescribe la s. 27 del Copyright, Designs, and Patents Act 1988:
"(1) In this Part "infringing copy", in relation to a copyright work, shall be construed in accordance with this section.
(2) An article is an infringing copy if its making constituted an infringement of the *copyright* in the work in question.
(3) An article is also an infringing copy if : (a) it has been or is proposed to be imported into the United Kingdom, and (b) its making in the United Kingdom would have constituted an infringement of the copyright in the work in question".

98. "Mr Kime relies on this definition in two ways. First, he says that an infringing copy must be an 'article'. In other words it must be shown that, at the relevant time, Mr Ball knew or had reason to believe that the Messiah 2 chip would be used to make articles which are infringing copies. He says that no such articles exist here. The Messiah 2 chip is not used for making unauthorized copies of the CD or DVD on which the PS2 game is supplied by Sony. Nor is it argued that an imported *authentic*, but 'foreign', PS2 game is either an infringing copy or made by use of the Messiah 2 chip […]": *Sony v Gaynor David Ball and other*, High Court of Justice, Chancery division, Mr. Justice Laddie, 19 July 2004 (num. 12).

pyright de Sony y la creación de copias infractoras. "Cuando el juego es insertado en la consola, el programa y otros trabajos creativos (o parte sustancial de ellos) son leídos del CD o DVD y copiados en la memoria chip RAM situada en la consola. Esto es un acto de reproducción." El abogado defensor contrarreplicó argumentando que si bien era cierto que el proceso descrito encerraba un acto de reproducción, no lo era que los datos digitales reproducidos del CD o DVD contenido en la RAM fueran una copia infractora. Señaló el hecho de que "la copia de la obra en la RAM sólo existe por una pequeña fracción de segundo". Añadió que ello es "muy efímero para convertir la RAM en una copia infractora". Tal reproducción es apenas "una creación temporal producida durante un acto dinámico de copiado". Según una interpretación sistemática de varias normas inglesas, afirmó el abogado defensor, la palabra "artículo" (que es el primer elemento del concepto de copia infractora según la s. 27 citada atrás) fue reservada por el legislador a "sustancias tangibles". Agregó que un chip "RAM que contiene una copia del todo o parte sustancial de la obra de Sony protegido por el *copyright*, no es tal sustancia tangible"[99].

El juez determinó que "no puede haber duda de que los chips de silicona son artículos" y agregó que "el hecho de que no contenía la copia antes y no la contenga después no altera su característica física [de tangible] cuando sí la contiene. [El chip RAM] siempre es un artículo pero una copia infractora por un corto periodo de tiempo. No hay nada en la legislación que sugiera que un objeto que contiene una copia de una obra protegida por el *copyright,* aun si es sólo de manera efímera, por ello no debe ser tratado como un artículo. Por el contrario, la definición en la s. 27 señala el instante de la realización de la copia como crucial para la determinación de si es o no un artículo infractor. Un artículo se convierte en un artículo infractor por razón de la forma en que es hecho. Si es un artículo infractor según la definición de la legislación debe ser determinado con referencia a ese momento. No importa si permanece en ese estado, teniendo en cuenta que retención como una copia no es parte de la definición"[100].

99. "Sony alleges that use of either of these, enabled by the Messiah 2 chip, inevitably results in infringement of Sony copyright and the creation of infringing copies. When the game is inserted into the console, the program and other creative works (or substantial parts of them) are read from the CD or DVD and copied into a Random Access Memory chip ('RAM') in the console. This is an act of reproduction. Mr Kime does not dispute that. Furthermore the RAM containing the reproduced digital data from the CD or DVD is an infringing copy. This is disputed by Mr Kime. He points to the fact that the copy of the copyright works in RAM only exist for a small fraction of a second. He says that that is far too ephemeral to turn the RAM into an infringing copy. He says that a copy which lasts for such a short period is not an article. It is a temporary creation produced during a dynamic act of copying. He draws my attention to the Obscene Publications Act 1959, the Factories Act 1937, the Supply Powers Act 1975, the Aviation Security Act 1982, the Sale of Food and Drugs Act 1875 and the Prison Act 1865 to illustrate different ways in which the word "article" has been used in legislation. He argues that the legislature only uses the word 'article' in relation to what he calls 'tangible substances'. He says that a RAM chip containing a copy of the whole or a substantial part of Sony's *copyright* works is not such a tangible substance": *Sony v Gaynor David Ball and other*…, cit.

100. "I do not accept this argument. The silicon RAM chip is an article. When it

El segundo argumento del abogado defensor respecto de la ausencia de conocimiento del demandado de que con el Messiah se producirían copias infractoras es el siguiente: Mr. Ball exporta aproximadamente el 90% de los chips Messiah 2 son exportados para clientes extranjeros. Tales, una vez exportados, son instalados en consolas PS2 fuera del país. "Aun si son usados para ejecutar copias no licenciadas de juegos de PS2 o juegos auténticos pero que han sido importados paralelamente de un país que uso un sistema de color para TV 'extranjero', el copiado en el RAM ocurre cuando la consola está localizada, principalmente en un país extranjero"[101].

De nuevo, el abogado defensor señaló "el hecho de que bajo la s. 296 (en su forma original) los derechos de Sony sólo son infringidos si el demandado conoce o tiene razones para creer que el chip Messiah 2 'será usado para hacer copias infractoras' ". Sin embargo, bajo la s. 27(2), un artículo (en este caso la copia transitoria en el RAM) es sólo una copia infractora si "su 'elaboración constituyó una infracción del *copyright* en la obra en cuestión' o, bajo la sección 27(3) si 'el artículo ha sido o se pretende importar al Reino Unido'"[102].

La referencia al "*copyright*" en aquella subsección (27[2]) debe entenderse que lo hace al *copyright* del Reino Unido. En relación con la última subsección, dijo también la defensa, los demandantes no alegaron que por lo menos una de las consolas a las cuales los chips exportados les fueron instalados hubiese sido importada de regreso al Reino Unido. El abogado agrega que se debe deducir que la venta de chips en el mercado externo no resultará en la creación de copias infractoras (respecto de la ley del Reino Unido, se insiste). Por tal razón, el comerciante que en el Reino Unido comercia chips que "serán o podrán terminar en el extranjero no puede tener el conocimiento o creencia de que será usado para hacer copias infractoras", tal como es requerido por la s. 296(2)[103].

contains the copy data, it is also an article. The fact that it did not contain the copy before and will not contain the copy later does not alter its physical characteristics while it does contain a copy. It is always an article but it is only an infringing article for a short time. There is nothing in the legislation which suggests that an object containing a copy of a *copyright* work, even if only ephemerally, is for that reason to be treated as not an article. On the contrary, the definition in s 27 points to the instant of making of the copy as crucial to the determination of whether or not it is an infringing article. *An article becomes an infringing article because of the manner in which it is made. Whether it is an infringing article within the meaning of the legislation must be determined by reference to that moment. It matters not whether it is remains in that state, since retention as a copy is no part of the definition in the section*": *Sony v Gaynor David Ball and other…*, cit. (cursivas agregadas).

101. "Mr Kime's second argument in relation to infringing copies runs as follows. Mr Ball claims that some 90% of Messiah 2 chips are exported to foreign customers. For present purposes it should be assumed that this factual assertion is correct. Those chips will be installed in PS2 consoles abroad. Even if they are used, as they must be expected to be, for running unlicensed copies of PS2 games or authentic games which have been parallel imported from a country using a 'foreign' colour television system, the copying into RAM occurs where the console is located, namely in the foreign country […]": *Sony v Gaynor David Ball and other…*, cit.

102. Ídem.

103. "Mr Kime's second argument in relation to infringing copies runs as follows. Mr

En otras palabras, el abogado planteó que el demandado no podía tener conocimiento de que el chip Messiah 2 sería usado para producir copias infractoras por el hecho de que la "infracción" debe entenderse en relación con la legislación del Reino Unido, a la par que la mayoría de las copias en RAM ocurrían en el extranjero por efecto de los chips exportados.

Esta interpretación, en líneas generales, fue aceptada por el juez del caso[104].

Este elemento hace difícil la aplicación de la disposición, tal como lo resaltó el abogado de Sony, quien sugirió que si la interpretación propuesta por la defensa (luego acogida por el juez) fuese correcta, "el comerciante estaría en posibilidad de asentarse en un país y conducir exclusivamente un mercado de exportación. El resultado sería

Ball claims that some 90% of Messiah 2 chips are exported to foreign customers. For present purposes it should be assumed that this factual assertion is correct. Those chips will be installed in PS2 consoles abroad. Even if they are used, as they must be expected to be, for running unlicensed copies of PS2 games or authentic games which have been parallel imported from a country using a 'foreign' colour television system, the copying into ram occurs where the console is located, namely in the foreign country. Once again, Mr Kime points to the fact that under s 296 in its original form, Sony's rights are only infringed if Mr Ball knows or has reason to believe that the Messiah 2 chip 'will be used to make infringing copies'. However, under s. 27(2) an article (in this case the transient copy in ram) is only an infringing copy 'if its making constituted an infringement of the copyright in the work in question' or, under s 27(3) if 'the article' has been or is proposed to be imported into the United Kingdom. The reference to copyright in the former subsection must be a reference to United Kingdom copyright. Mr Mellor accepts that. In relation to the latter subsection it is not pleaded or suggested that any of the consoles to which exported Messiah 2 chips are fitted will be imported back into this country. Mr Mellor accepts that also. Mr Kime argues that it must follow that the sale of the chips into the export market will not result in the creation of infringing copies. For that reason, the trader here who deals with chips which will or might end up abroad can not have the knowledge or belief that it 'will be used to make infringing copies' as required by s 296(2)": Sony v Gaynor David Ball and other…, cit.

104. 81 "How does this impact on Sony's claim? It should be noticed that the section does not prohibit export of this kind of device. Therefore Sony's claim under this section is in respect of all the Messiah 2 chips which are imported into this country and are exploited here whether by way of sale, offer or exposure for sale, advertising for sale and possession for commercial purposes. Insofar as Mr Ball has sold Messiah 2 chips here, he has breached Sonys rights under the section. In respect of those products, Mr Ball knows or has reason to believe that they will be used to make infringing copies. On the other hand the position in relation to all the rest of his stock and his other commercial activities, is less straightforward. Assume that he has 100 chips and he advertises them for sale both to UK and Continental customers, for example on the internet. When he effects a sale to the former, he breaches the section. But what is the position before that? If the chips are suitable for sale to any customer in any country, it must follow that, prior to receipt of an order, Mr Ball does not know whether an individual chip will be sold and installed here or abroad. If that is so, then at the time of advertising he does not know or have reason to believe that any particular chip 'will' be used to make infringing copies as required by s 296. All that he knows is that it might be so used. He does not breach Sony's rights. The same result may well apply to activities such as manufacturing and having in his possession for commercial purposes. In each case what will count is whether or not he knew that the chips he was dealing with were for supply to a UK or a foreign customer. For example, possession of stock which he knows is destined for the UK market would be a breach but possession of stock which is designed to service future customers in any market or only export markets would not. It follows that Mr Ball's liability in relation to these activities is dependent on the particular facts of each type of commercial activity in respect of which Sony complains. It is not a matter which can be resolved on a summary application": *Sony v Gaynor David Ball and other*…, cit.

que compañías en la posición de Sony estarían obligadas a demandar a los compradores en el país de importación. Los comerciantes estarían fuera de alcance"[105].

La solución a este problema de aplicación de la norma puede ser ya sea redefinir el contenido del elemento subjetivo de potencial infractor o eliminar cualquier referencia a un elemento subjetivo en la configuración de la infracción.

El primer camino fue la interpretación sugerida por el abogado de Sony. En efecto, señaló que "el propósito legislativo tras la s. 296(2) es atrapar a aquellos que conocen o tienen razones para creer que el equipo que están comercializando será usado para vencer una medida de protección contra la copia [léase, como medida tecnológica]. De tal manera, *si el uso causa o no causa infracción del* copyright *y, si tal cosa ocurre, dónde, es de poca monta*"[106] (cursivas agregadas). Igual a lo propuesto por este abogado, la legislación australiana centró este elemento subjetivo en el conocimiento de que el equipo es un dispositivo de elusión de una medida tecnológica, sin importar el conocimiento del sujeto de (o las razones para creer) que será utilizado para infringir el *copyright* sobre la obra.

El segundo camino es eliminar cualquier referencia de un elemento subjetivo en la configuración, tal como lo hizo la reforma inglesa de 2003. Respecto de la supresión de tal elemento subjetivo, el juez del caso que se viene comentando señaló: "[…] debe ser señalado que ésta [se refiere a la sección 296ZD, que es posterior a la mencionada reforma] crea una hipótesis de responsabilidad objetiva. Mr. Ball no puede escapar de su responsabilidad demostrando que no conocía o no tenía razones para creer que los chips Messiah 2 serían usados para elaborar copias infractoras de las obras de Sony protegidas por el *copyright*. Por otro lado, las definiciones muestran que el propósito principal de los sistemas de protección de copia [léase medida de protección] debe ser *proteger la obra sujeta a copyright* con miras a prevenir infracciones al *copyright*. Sin embargo, hay importantes diferencias entre estas normas [296ZD y 296ZF] y aquellas bajo la s. 296. Acá, la referencia a la *protección del copyright* y, por ende, a la supresión de la infracción, es completamente restringida a la definición de 'medida tecnológica de protección'. En otras palabras, para determinar si el sistema de Sony es uno protegido por esas normas, es necesario determinar si es diseñado en el curso normal de su operación para prevenir el uso no autorizado la obra de Sony sujeta a *copyright* en una forma que equivaldría a una infracción del *copyright* […]" (traducción libre, cursivas añadidas)[107]. En síntesis, la relación que la medida

105. "The merchant would be able to sit in one country and conduct an exclusively export trade. The result would be that companies in Sony's position would be obliged to sue customers in the country of importation. The merchant would be out of reach."

106. He argues that the legislative intent behind s 296(2) is to catch those who know or have reason to believe that the equipment in which they are trading is to be used to overcome copy-protection. As such, whether or not the use of the equipment causes infringement of copyright and, if so, where, is of little significance.

107. "It should be noticed that this creates a tort of strict liability. Mr Ball cannot escape from liability by showing that he did not know or have reason to believe the Messiah 2 chips would be used to make infringing copies of Sony copyright works. On the other hand the definitions show that the main purpose of the copy protection system must be to protect copyright work so as to prevent infringements of copyright.

tecnológica debe tener con el *copyright* no deriva ya del conocimiento del sujeto, sino de su definición misma.

A modo de síntesis: el conocimiento es un requisito para configurar esta modalidad de infracción, aunque no está presente en algunas legislaciones como la estadounidense. El contenido del conocimiento puede ser, según disponga la ley, que el objeto es un dispositivo de elusión o que el uso que se le dará al dispositivo será para realizar copias no autorizadas. Este último, según vimos en la jurisprudencia, presenta dificultades en su interpretación.

C. PRESTACIÓN DE SERVICIOS

Para la legislación estadounidense y para la inglesa, los presupuestos son los mismos señalados atrás. Así como ocurre con las conductas en relación con un dispositivo, la legislación australiana agrega el elemento subjetivo del conocimiento de –o el deber de razonablemente conocer– que el servicio es para la elusión de una medida tecnológica de protección.

IV. EXIMENTES DE RESPONSABILIDAD POR ELUSIÓN DE UNA MEDIDA TECNOLÓGICA

Un derecho subjetivo no es sólo un poder jurídico atribuido a un sujeto de derecho: también refleja una solución política dada por el legislador a un real o potencial conflicto de intereses.

El derecho subjetivo de ciertos sujetos a reclamar una reparación respecto de quien realiza conductas efectivas o potencialmente elusivas también es una solución de un conflicto de interés: el interés (principalmente) económico del autor o de su licenciatario (o de los otros posibles titulares, según vimos atrás) frente a los intereses de la comunidad (el acceso al conocimiento, al arte; el desarrollo tecnológico y económico; la defensa y la seguridad nacionales, etc.) y de particulares.

El interés de los primeros, al conferírsele estatus de derecho subjetivo, se convierte en la regla general, en lo llamado a ser respetado y a prevalecer. Todos los intereses (de la comunidad y particulares) contrarios al interés de aquéllos están llamados, en principio, a estar subordinados; las acciones encaminadas a desarrollar esos intereses, expuestas a ser calificadas de antijurídicas; sus ejecutores, de infractores; sus patrimonios, a servir como garantía de la reparación debida; y sus libertades, a ser restringidas por la ley penal.

However there are important differences between these provisions and those under s 296. Here, the reference to protecting copyright and, by implication, the suppression of infringement is all restricted to the definition of 'technological measures'. In other words, to determine whether the Sony system is one protected by these provisions, it is necessary to determine whether it is designed in the normal course of its operation to prevent unauthorized use of Sony's copyright work in a way which would amount to an infringement of copyright": Sony v Gaynor David Ball and other…, cit. (num. 39).

Ahora bien: estos intereses en principio no prevalecientes (de la comunidad o particulares) cumplen una función socialmente útil. Esta utilidad da lugar a que sobre esos intereses (y las conductas que los persiguen) se dé un nuevo juicio legislativo cuyo objetivo es avalar aquellos que, aunque inicialmente prohibidos, representan para la sociedad una utilidad mayor que la que representa la satisfacción del interés protegido por la regulación de medidas tecnológicas (especialmente, la garantía de los derechos de propiedad intelectual en el entorno digital). De este juicio nacen las excepciones a la prohibición de eludir las medidas tecnológicas[108].

Los intereses de la comunidad y de particulares resaltan en las excepciones más comunes. El DMCA prevé excepciones a favor de los archivos, bibliotecas e instituciones educativas; de ciertas actividades del gobierno; para la realización de pruebas de seguridad; para la protección de menores y de datos personales; para la realización de actividades de ingeniería inversa.

La Biblioteca del Congreso, en ejercicio de una facultad atribuida por la s. 1201 del DMCA, exceptuó también de la prohibición de eludir medidas tecnológicas de protección las siguientes actividades: el "acceso a compilaciones de sitios de Internet bloqueados por programas de filtrado, conocidos como *censorware*"[109]; "los programas de computador protegidos por medidas tecnológicas a los que ya no se puede acceder en vista de que el dispositivo tecnológico no funciona bien o ha sufrido algún daño y bajo condición de que no pueda ser sustituido o reparado"[110]; "los programas de computador y juegos de video distribuidos en formatos que se han convertido en obsoletos y que requieren el *hardware* o medio físico original para poder funcionar"[111]; "obras literarias distribuidas en formato *e-book*, en las cuales el editor ha deshabilitado las funciones de lectura en voz alta o la posibilidad de usar lectores de pantalla para llevar el texto a una forma especializada como el Braille para brindar acceso a los ciegos"[112].

Vale agregar que la norma australiana de 2006 expresamente excluyó de protección a las medidas tecnológicas cuyo objeto sea segmentar regionalmente el mercado, como serían aquellas que incluyen los CD o DVD que sólo permiten la reproducción de éstos en una consola correspondiente a la zona para la cual fueron distribuidos[113].

108. En el DMCA estas excepciones sólo aplican a la primera modalidad de infracción, *la acción de eludir la medida*, mas no a las otra modalidades. MARKS y TURNBULL señalan: "puesto que, por su naturaleza, los dispositivos y los servicios no se pueden limitar a usos particulares, las excepciones a las leyes contra la elusión no parecen muy adecuadas para estos dispositivos y servicios" (Documento OMPI…, cit., p. 10).

109. RODRÍGUEZ MORENO. *La era digital y las excepciones y limitaciones al derecho de autor*, cit., p. 186. Agrega: "El objeto de estos programas es impedir el acceso de menores y otros usuarios a ciertos dominios, sitios de internet o porciones de sitos cuyo contenido es poco adecuado para estas personas".

110. Ibíd., p. 187.

111. Ídem.

112. Ibíd., pp. 187-188.

113. "Subsection 10(1) but does not include such a device, product, technology or component to the extent that it: […] (iii) if the work or other subject-matter is a cinematograph film or computer program (including a computer game)—controls geographic

Una exposición exhaustiva y completa de cada una de las excepciones requiere un escrito aparte, dada la importancia, la extensión y el nivel de complejidad de la tarea. Por tal razón, en este punto simplemente se ha mostrado la existencia de otros intereses socialmente útiles que han ameritado crear excepciones a la prohibición general y a la responsabilidad por eludir medidas tecnológicas.

V. CONCLUSIONES

– La regulación sobre medidas tecnológicas de protección –como tales– tiene su origen en los tratados OMPI de mediados de los años noventa que hemos citado. No obstante, en Estados Unidos, por vía jurisprudencial ya existían antecedentes de protección jurídica sobre tales medidas (*Sega v Maphia*).

– La función práctica que, en principio, pretende cumplir la regulación sobre medidas tecnológicas es la de reforzar las acciones (materializadas en medidas tecnológicas de protección) de los propietarios de contenido para mantener sus derechos de propiedad intelectual vigentes en el nuevo entorno digital. Pese a lo anterior, hoy en día las funciones de las medidas tecnológicas parecen haber trascendido más allá de la propiedad intelectual[114] y del derecho mismo[115]. Este interesante punto no fue tratado por trascender las fronteras de lo que nos hemos propuesto para este artículo.

– En líneas generales, la regulación sobre medidas tecnológicas de protección y su elusión en los sistemas de *copyright* cuenta con unos elementos estructurales identificables: el concepto de medida tecnológica; sus formas de elusión y las excepciones a la prohibición de, y a la responsabilidad por, eludir la medida. El concepto de medida de protección tecnológica es el que presenta más dificultades de interpretación, especialmente en lo relacionado con las finalidades que debe cumplir y la noción de efectividad. Problemática, aunque no tanto como lo anterior, es la interpretación de los estados de conocimiento que debe tener la elusión.

– La regulación de medidas tecnológicas tiene y debe tener en cuenta otros intereses (de la comunidad y de particulares) distintos de la garantía de los derechos de propiedad intelectual en el entorno digital. De lo contrario, el desarrollo del comercio electrónico, el acceso al conocimiento, la función social de la propiedad intelectual y otros caros intereses podrían verse perjudicados.

market segmentation by preventing the playback in Australia of a non-infringing copy of the work or other subject-matter acquired outside Australia [...]".

114. CASAS VALLÉS. "Copia privada y medidas tecnológicas: el caso 'Mulholland Drive' ", cit. El autor parece sugerir que la propiedad intelectual sería reemplazada en un futuro por una sinergia entre contratos, medidas tecnológicas y legislación sobre elusión.

115. Ver el Children Internet Protection Act (CIPA) y su sentencia de constitucionalidad (*United States* et al. *v. American Library Association, Inc.*, et al.). Por medio de esta sentencia estadounidense se avala la imposición a bibliotecas y escuelas de aplicar medidas tecnológicas que neutralicen el acceso a contenidos ofensivos para menores. Esta regulación parece mostrar que las medidas tecnológicas parecen escapar del ámbito meramente jurídico para garantizar fines eminentemente morales.

– La exposición que se ha presentado en el escrito sobre la configuración legislativa de las medidas tecnológicas y su elusión es una base fundamental y necesaria para otras discusiones, unas de interés dogmático, otras de interés político.

Son de interés dogmático la discusión sobre la ubicación sistemática de la regulación sobre medidas dentro del derecho y por ende su naturaleza (¿es una forma de derecho propietario?, ¿es un caso legalmente típico de responsabilidad civil?, en cualquiera de los dos casos, ¿tiene cabida dentro del sistema de la propiedad intelectual?); la discusión sobre los retos que plantea para la pervivencia de la propiedad intelectual a futuro inmediato y mediato; y, por último, la discusión sobre la *necesidad jurídica* de una regulación específica relacionada con la elusión (¿se pueden lograr los mismos efectos mediante las normas generales de propiedad intelectual o de responsabilidad civil?).

De interés político es la discusión sobre el carácter nocivo de una protección jurídica a tales medidas para el desarrollo del comercio electrónico, el conocimiento y otros intereses, tal como ya se ha dicho. En últimas, es una discusión sobre la *conveniencia* de una protección de medidas tecnológicas, inevitablemente permeada por consideraciones constitucionales y de los intereses propios del país en cuestión.

BIBLIOGRAFÍA

Casas Vallés, Ramón. "Copia privada y medidas tecnológicas: el caso 'Mulholland Drive'", en *Derecho de Autor*, Cerlac-Unesco-Univesidad de los Andes, n.º 1, enero-junio de 2007.

Copinger & Skone James. *On Copyright*, x ed., Sweet and Maxell, 1989.

Hinze, Gwen. "Seven Lessons from a Comparison of the Technological Protection Measure Provisions of the FTAA, the DMCA, and recent bilateral Free Trade Agreements, Documento de Electronic Frontier Foundation", en [www.eff.org/pages/seven-lessons-comparison-technological-protection-measure-provisions].

Hollaar, Lee. *A Bad Trade - Will Congress Unwittingly Repeal the Digital Millennium Copyright Act and Violate our Trade Treaties?*, Institute for policy Innovation, Center for Technology freedom, 2006.

Hollaar, Lee. *Still "Bad": A Critique of the Latest Attempt to Gut the DMCA*, Institute for policy Innovation, Center for Technology Freedom, 2008.

Marks, Dean S. y Bruce H. Turnbull. Marks y Turnbull. Documento OMPI. *Las medidas tecnológicas de protección: el punto de encuentro de la tecnología, el derecho y las licencias comerciales*, s. d.

Ricketson, Sam y Jane C. Ginsburg. *International Copyright and Neighboring Rights*, 2.ª ed., vol. II, Oxford University Press, 2006.

Rodríguez Moreno, Sofía. *La era digital y las excepciones y limitaciones al derecho de autor*, Bogotá, Universidad Externado de Colombia, 2004.

Samuelson, Pamela. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised", publicado originalmente

en 14 *Berkeley Technology L. J.* 519, 521 & 531-32, 1999, disponible en [http://people.ischool.berkeley.edu/~pam/papers/Samuelson.pdf].

SCHECHTER, ROGER E. y JOHN R. THOMAS. *Intellectual property the law of copyrights, patents and trademarks*, Thomson-West, 2003.

TIMIRAOS, NICK. "Obama Vows Opposition to Colombia Trade Deal", en *The Wall Street Journal*, 4 de abril de 2008, en [http://blogs.wsj.com/washwire/2008/04/02/obama-vows-opposition-to-colombia-trade-deal/?mod=wsjblog].

VÄLIMÄKI, MIKKO. "Continúa el Hacking, Sentencia del 25 de mayo de 2007, Corte del Distrito de Helsinki, Finlandia" (trad. JHONNY ANTONIO PABÓN CADAVID), en *Revista del Centro Colombiano de Derecho de Autor*, n.º 12, octubre de 2007.

CASOS

Chamberlain Group, Inc. v. Skylink Techs., Inc., 2004 U. S. App. Lexis 18513, at *52 (Fed. Cir. Aug. 31, 2004).

CoxCom, Inc v Jon Chaffee, United States Court of Appeals for the First Circuit, August 4, 2008.

Lexmark International, Inc v Static Control Components, Inc, United States Courts of Appeals – For the Sixth Circuit, October 26, 2004.

Neil Stanley Higgs v The Queen [2008], EWCA Crim. 1324.

RealNetworks Inc. v Streambox, Inc., 2000 U. S. Dist. Lexis 1889 (W. D. Wash. Jan. 18, 2000).

Sony v Gaynor David Ball and other, High Court of Justice, Chancery division, Mr. Justice Laddie, 19 July 2004 (num. 36).

Sega Enterprises, Ltd. v. Maphia, 857 F. Supp. 679 (N. D. Cal. 1994).

Sega Enterprises, Ltd. v. Maphia, 948 F. Supp. 923 (N. D. Cal. 1996).

Sony v Gaynor David Ball and other, High Court of Justice, Chancery division, Mr. Justice Laddie, 19 July 2004 (num. 42-43).

Stevens v Kabushiki Kaisha Sony Computer Entertainment [2005] HCA 85 (6 October 2005), num. 110.

United States v. Elcom Ltd, 203 F. Supp.2d 1111 (N. D Cal. May 8, 2002).