



**VNiVERSiDAD
D SALAMANCA**

CAMPUS DE EXCELENCIA INTERNACIONAL

*TRABAJO DE FIN DE GRADO
GRADO EN INGENIERÍA INFORMÁTICA
FACULTAD DE CIENCIAS*

Curso 2022/2023

LA PROTECCIÓN JURÍDICA DEL SOFTWARE

THE LEGAL PROTECTION OF SOFTWARE

Autor: Ángel Pescador Cantos Correo: angelpc99@usal.es

Tutora: Prof. Dra. Carmen Rosa Iglesias Martín

Julio 2023

Dña. Carmen Rosa Iglesias Martin, profesora del Departamento de Derecho Privado, área de Derecho Civil de la Universidad de Salamanca.

CERTIFICA:

Que el trabajo titulado “La protección jurídica del software” ha sido realizado por D. Ángel Pescador Cantos con DNI 70966452K y constituye la memoria del trabajo realizado para la superación de la asignatura Trabajo Fin de Grado de la Titulación del Grado en Ingeniería Informática de esta Universidad.

Y para que así conste a todos los efectos oportunos.

En Salamanca a 8 de junio de 2022

Firmado por IGLESIAS MARTIN, CARMEN ROSA (FIRMA)

el día 08/06/2023 con un certificado emitido por AC
DNIE004

Resumen

La protección jurídica del software incluye las normas y regulaciones que salvaguardan los derechos de propiedad intelectual relacionados con el desarrollo y uso de los programas informáticos.

El software se define como un conjunto de instrucciones lógicas que permiten a un dispositivo electrónico llevar a cabo funciones específicas. Puede clasificarse en software de sistema y software de aplicación.

La Ley de Propiedad Intelectual, que otorga derechos exclusivos al creador del programa, rige la protección legal del software en España. A nivel de la Unión Europea, las directivas como la Directiva de Software y la Directiva de Derechos de Autor ofrecen el mismo nivel de protección en todos los estados miembros.

La piratería de software y la violación de los derechos de propiedad intelectual son problemas comunes. La piratería de software se refiere a la reproducción y distribución no autorizadas de programas protegidos. El uso de software sin licencia, la copia ilegal y la falsificación son ejemplos de piratería.

Estas prácticas ilegales tienen un impacto negativo significativo en la innovación y resultan en pérdidas de ingresos para los titulares de derechos. Los sistemas de gestión de licencias, las tecnologías antipiratería y las acciones legales son solo algunas de las herramientas utilizadas en la lucha contra la piratería.

El objetivo de la fiscalización y las sanciones es garantizar el cumplimiento de las leyes de protección del software. Las autoridades competentes pueden procesar a aquellos que violan los derechos de propiedad intelectual y someterlos a multas y penas de prisión, además de realizar inspecciones.

Existen muchos ejemplos reales de violaciones de propiedad intelectual en el software. Por ejemplo, la distribución y apropiación ilícita de software comercial, la modificación no autorizada de software de código abierto y la venta de copias piratas en línea. Varios tribunales han emitido decisiones relevantes en estos casos, estableciendo precedentes legales y protegiendo los derechos de los titulares de software. Uno de los ejemplos más destacados es la demanda de Microsoft contra los distribuidores de software pirata.

En conclusión, preservar los derechos de propiedad intelectual en este campo requiere la protección jurídica del software. Los marcos legales establecen derechos y medidas para combatir la piratería en España y la Unión Europea. Hay consecuencias graves para aquellos que infringen los derechos de propiedad intelectual en el software, pero se pueden utilizar herramientas tanto tecnológicas como legales para prevenir y sancionar estas prácticas ilegales.

Palabras clave: Protección jurídica del software, software, ley, falsificación, piratería, derechos de autor, derechos de propiedad intelectual, acciones legales, software sin licencia, sentencias, marco legal.

Abstract

The legal protection of software includes the rules and regulations that safeguard intellectual property rights related to the development and use of computer programs.

Software is defined as a set of logical instructions that enable an electronic device to perform specific functions. It can be classified into system software and application software.

The Intellectual Property Law, which grants exclusive rights to the creator of the program, governs the legal protection of software in Spain. At the European Union level, directives such as the Software Directive and the Copyright Directive offer the same level of protection in all member states.

Software piracy and the violation of intellectual property rights are common issues. Software piracy refers to the unauthorized reproduction and distribution of protected programs. Examples of piracy include the use of unlicensed software, illegal copying, and counterfeiting.

These illegal practices have a significant negative impact on innovation and result in revenue loss for rights holders. License management systems, anti-piracy technologies, and legal actions are just a few of the tools used in the fight against piracy.

The aim of enforcement and penalties is to ensure compliance with software protection laws. Competent authorities can prosecute those who violate intellectual property rights and subject them to fines and imprisonment, as well as conduct inspections.

There are many real-world examples of intellectual property violations in software. For instance, the unauthorized distribution and appropriation of commercial software, unauthorized modification of open-source software, and the sale of pirated copies online. Several courts have issued relevant decisions in these cases, establishing legal precedents and protecting the rights of software holders. One notable example is Microsoft's lawsuit against distributors of pirated software.

In conclusion, preserving intellectual property rights in this field requires the legal protection of software. Legal frameworks establish rights and measures to combat piracy in Spain and the European Union. There are severe consequences for those who infringe intellectual property rights in software, but technological and legal tools can be used to prevent and sanction these illegal practices.

Keywords: Legal protection of software, software, law, counterfeiting, piracy, copyright, intellectual property rights, legal actions, unlicensed software, court decisions, legal framework.

Índice

Resumen.....	2
Abstract	3
1. Introducción	5
1.1 Presentación del tema.....	5
1.2 Objetivos	5
1.3 Justificación de la relevancia del tema	6
2. Conceptos básicos	6
2.1 Definición de software	6
2.2 Tipos de software	7
2.3 Propiedad intelectual y software	10
2.3.1 Propiedad intelectual y derechos de autor en el software libre	11
2.4. Licencias de software	11
3. Protección jurídica del software.....	14
3.1. Marco legal del software en la Unión Europea	14
3.2. Marco legal del software en España.....	19
3.3. Protección de los derechos de autor en el software.....	22
3.4. Protección de las patentes de software	24
3.5. Protección de las marcas en el software	25
4. Piratería y violación de derechos de propiedad intelectual.....	26
4.1. Concepto de piratería informática	26
4.2. Tipos de piratería.....	27
4.3. Daños causados por la piratería	29
4.4. Herramientas contra la piratería	32
5. Fiscalización y sanciones	36
5.1. Fiscalización del software en España	36
5.2. Sanciones por la violación de derechos de propiedad intelectual en el software	39
6. Casos prácticos.....	41
6.1. Ejemplos de casos de violación de derechos de propiedad intelectual en el software	41
6.2. Sentencias relevantes en materia de protección del software	41
7. Conclusiones.....	42
7.1. Recapitulación de los aspectos más relevantes tratados en el trabajo.....	42
7.2. Reflexiones y propuestas de mejora	43
7.3. Posibles líneas de investigación futura.....	44
8. BIBLIOGRAFIA.....	46

1. Introducción

1.1 Presentación del tema

En este trabajo abordaremos el tema de la protección jurídica del software, para ello, analizaremos temas relevantes para la protección de los derechos de autor para el creador del software, ya que, este último es un elemento indispensable en nuestras vidas hoy en día, tanto en la vida de las personas físicas como en la de las personas jurídicas.

El software es una creación intelectual, lo que se refiere a ¹toda producción en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión. En este trabajo abordaremos temas como la propiedad intelectual, las leyes que protegen el software, los mecanismos que poseemos para su protección y las estrategias para prevenir la piratería y la violación de los derechos de autor.

En primer lugar, haremos una introducción del concepto de software, así como la relevancia que tiene en la actualidad. Para ello nos serviremos del análisis de la propiedad intelectual y su relación con el software, haciendo hincapié en las formas de protección que existen, como el derecho de autor y las patentes.

1.2 Objetivos

En este apartado, dividiremos los objetivos en dos, diferenciando entre principales y secundarios.

Objetivo principal: analizar el marco jurídico que protege el software tanto a nivel nacional como internacional.

Objetivo secundario: identificar leyes, normativas y tratados relevantes en la materia.

Objetivo principal: Identificar los diferentes tipos de protección que existen para el software, incluyendo el derecho de autor, patentes, marcas, secretos comerciales y otros mecanismos de propiedad intelectual.

Objetivo secundario: Evaluar las ventajas y desventajas de cada uno de los mecanismos de protección para el software.

Objetivo secundario: Analizar casos prácticos de protección del software, tanto en el ámbito nacional como internacional para entender cómo se aplican los distintos mecanismos de protección.

Objetivo principal: Evaluar las posibilidades de innovación en el ámbito del software.

¹ Artículo 2 de la Convención de Berna para la Protección de las Obras Literarias y Artísticas

1.3 Justificación de la relevancia del tema

El software es un bien inmaterial que requiere protección o tutela jurídica por razones de justicia y de política económica.

Las instrucciones que componen un programa informático son el resultado del ingenio humano y están destinadas a lograr un resultado específico a través de su ejecución por un ordenador. Aunque requieren de un soporte físico, no se confunden con él, sino que pueden operar simultáneamente en un número ilimitado de ordenadores o estar almacenados en un número también ilimitado de copias. Por esta razón, es necesario proporcionar una protección efectiva tanto para los programas como para sus creadores.

La protección jurídica del software se consigue a través de diversas formas de propiedad intelectual, tales como el derecho de autor, la patentes, los modelos de utilidad, ente otros. La forma más común para el software es el derecho de autor, pues se protege la expresión original del software, incluyendo su código y su documentación.

La protección jurídica del software es esencial porque reconoce y protege los derechos de propiedad intelectual de los creadores de software, permitiéndoles obtener beneficios económicos y mantener el control sobre el uso y la distribución de su obra. Además, la protección jurídica del software puede contribuir a prevenir la piratería y la infracción de los derechos de autor, lo que a su vez fomenta la innovación y el desarrollo tecnológico.

En resumen, la protección jurídica del software es esencial para fomentar la innovación y el desarrollo en el campo del software, proteger los derechos de propiedad intelectual de los creadores de software y prevenir la piratería y la violación de derechos de autor.

2. Conceptos básicos

2.1 Definición de software

Según lo que encontramos en la Real Academia de la Lengua Española (en adelante, RAE), definimos software como: ²“Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.”

El software, a nivel jurídico, se considera como una obra intelectual protegida por el derecho de autor, siempre y cuando cumpla con los requisitos establecidos por la ley. Al ser una creación individual, el software expresa una idea a través de un determinado lenguaje y su autor o autores tienen el derecho exclusivo de controlar su reproducción, distribución, modificación y comunicación pública.

Además, ³jurídicamente el software es considerado un bien intangible, susceptible de ser objeto de compraventa, licencia, cesión y otros tipos de transacciones comerciales y está sujeto a la

² Real Academia Española. (s.f.). Software. En Diccionario de la lengua española

³ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

protección de otras áreas del derecho, como el derecho de propiedad industrial, el derecho mercantil o el derecho de la competencia.

La definición jurídica del software es fundamental para garantizar la protección de los derechos de los autores, titulares y propietarios del software, y para su adecuada explotación y comercialización en el mercado.

"Software" en el campo de la ingeniería del software se refiere a los programas, aplicaciones y datos almacenados en un sistema informático que permiten su funcionamiento y uso. A diferencia del hardware, que se refiere a los componentes físicos de un sistema informático, el software es el componente lógico e intangible.

El software puede ser de varios tipos, como sistemas operativos, programas de aplicación, utilidades, juegos, entre otros. Los sistemas operativos son programas fundamentales que controlan los recursos de hardware de un ordenador y permiten que se ejecuten otras aplicaciones. Procesadores de texto, hojas de cálculo, navegadores web, reproductores de medios y otras aplicaciones son ejemplos de programas de aplicación. Herramientas de compresión de archivos, software antivirus, herramientas de copia de seguridad y otras utilidades son ejemplos de utilidades software. Las utilidades también ayudan en la administración del sistema o realizan tareas específicas.

El software puede ser creado por empresas, desarrollado por individuos o vendido bajo licencias específicas. También puede estar protegido por derechos de autor y la ley, por lo que su uso sin permiso puede infringir las leyes de propiedad intelectual.

En resumen, la programación en el campo de la ingeniería de software se refiere a los programas y datos que permiten el funcionamiento de los sistemas informáticos. Es un componente crucial de la tecnología que utilizamos a diario.

Por lo que visto todo lo anterior y respecto a lo que en este trabajo incumbe hemos de unir ambas definiciones, ya que en ellas encontraremos la respuesta más adecuada a nuestro fin. El software es un término utilizado en el ámbito legal para describir un producto intelectual protegido contra el robo mediante derechos de autor y otros tipos de propiedad intelectual. En el contexto de la informática, el software se refiere a los datos y programas que permiten el funcionamiento de los sistemas informáticos. Para comprender y regular el software, ambas perspectivas son necesarias e interconectadas.

2.2 Tipos de software

⁴Vamos a identificar varios tipos de software diferentes en función de su naturaleza y las normas legales que los rigen. Algunos de los más relevantes son:

1. Software libre: ⁵El software libre se refiere a programas de ordenador que otorgan a los usuarios la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. La filosofía del movimiento de software libre, que busca fomentar la colaboración, la transparencia y el acceso abierto al código fuente, sirve como base

⁴ Free Software Foundation. (s.f.). Categorías de software

⁵ Aldana, A. C. A., & Cuervo, M. C. (2009). Propiedad intelectual y derechos de autor en el software libre. Revista Virtual Universidad Católica del Norte, (28)

para estas libertades. Se caracteriza por estar disponible con una licencia de software libre, como la Licencia Pública General de GNU (GPL) o la Licencia MIT, que garantiza las libertades mencionadas anteriormente. Esto significa que los usuarios tienen derecho a adaptar y compartir el software con otros, así como la libertad de utilizarlo sin restricciones.

Además, el software libre fomenta una comunidad de desarrollo colaborativo en la que tanto los programadores como los usuarios pueden contribuir a la mejora del software y promueve la interoperabilidad, no depende de proveedores o tiene restricciones de uso como el software propietario.

2. ⁶Software propietario: Los programas informáticos que están restringidos en su uso, distribución y modificación por el titular de los derechos de autor o la empresa que los posee se conocen como software propietario. Por lo general, los usuarios de software propietario obtienen una licencia limitada para utilizar el software de acuerdo con los términos y condiciones establecidos por el titular de los derechos. El software propietario se caracteriza por ser cerrado, lo que significa que el código fuente no está disponible para su visualización o modificación por parte de los usuarios. Solo el titular de los derechos tiene acceso y control total sobre el código fuente. Las licencias de software, las claves de acceso y la protección anticopia son medidas de seguridad comunes utilizadas por los desarrolladores de software propietario para proteger su inversión y propiedad intelectual. Esto les permite controlar y adaptar el uso y la distribución del software.

A diferencia del software libre, los usuarios de software propietario no pueden acceder, modificar ni distribuir el código fuente. El software debe utilizarse de acuerdo con los términos de la licencia, y cualquier violación de esos términos podría resultar en acciones legales.

Es importante tener en cuenta que aunque el software propietario puede ofrecer ventajas en forma de soporte técnico, garantía de calidad y funcionalidades específicas, también restringe la libertad y transparencia del software.

3. ⁷Software de código abierto: El término "software de código abierto" se refiere a programas informáticos cuyo código fuente es libremente accesible al público y está disponible para su uso, modificación y distribución. El software de código abierto, a diferencia del software propietario, permite a los usuarios acceder, investigar, modificar y mejorar el código fuente de acuerdo con las licencias de código abierto aplicables. El software de código abierto se caracteriza por su transparencia y su filosofía colaborativa y de intercambio de conocimientos. Normalmente, se distribuye bajo licencias reconocidas como la Licencia Pública General de GNU (GPL), la Licencia MIT, la Licencia Apache, entre otras. Estas licencias garantizan la obligación de mantener el código fuente abierto y la libertad de uso, modificación y distribución del software. La comunidad de desarrollo de software de código abierto fomenta la colaboración, permitiendo a los usuarios y programadores contribuir con mejoras y correcciones de errores al software. Esto conduce al desarrollo y mejora rápida del software, así como a la creación de numerosos proyectos y aplicaciones de código abierto en diversas industrias.

⁶ Sánchez, R. G. (2003). Software libre vs. Software propietario: programando nuestro futuro. *Historia Actual Online*, (2), 9.

⁷ Cataldi, Z., & Salgueiro, F. (2007). Software libre y código abierto en educación. *Quaderns Digitals*, 48, 01-12.

Debido a su naturaleza abierta, el software de código abierto facilita que diferentes programas y sistemas trabajen juntos. Esto promueve la interoperabilidad y la compatibilidad entre sistemas.

En resumen, el software de código abierto brinda a los usuarios acceso, modificación y distribución del código fuente, lo que promueve la libertad y la transparencia. En el desarrollo de software, esto fomenta la innovación y la colaboración.

Es parecido al software libre pero tiene más restricciones llegando al punto de prohibir la redistribución de subproductos, siempre que se puedan publicar a cambio como parches o añadidos para el producto original.

4. ⁸Software patentado: Los programas informáticos que están protegidos por patentes se conocen como "software patentado". Una patente de software otorga al titular de la patente la propiedad exclusiva del software. Esto significa que otras personas no pueden utilizar, crear, vender o distribuir el software sin permiso del titular de la patente. El software de código abierto está protegido como propiedad intelectual, mientras que el software patentado no lo está. Los titulares de patentes de software pueden registrar sus invenciones en las oficinas de patentes correspondientes y obtener derechos legales para proteger su software. La patentabilidad del software puede variar según la legislación de cada país. Si bien no se reconocen patentes de software en todos los países, ciertos aspectos del software, como algoritmos o métodos específicos, son patentables en algunos lugares. En la industria, las patentes de software se utilizan con frecuencia para proteger la propiedad intelectual y la innovación. ⁹Sin embargo, también existen argumentos y controversias sobre su alcance y si realmente fomentan o dificultan la innovación en el campo del software.

En resumen, los programas informáticos que reciben derechos exclusivos sobre su uso y distribución mediante patentes se conocen como "software patentado".

5. Software de dominio público: Los programas informáticos que son de libre uso y distribución para el público en general y no están protegidos por derechos de autor se conocen como "software de dominio público". En otras palabras, el software que no tiene restricciones de derechos de autor se denomina software de "dominio público". El software que se encuentra en el dominio público no tiene limitaciones en cuanto a su uso, modificación o distribución impuestas por el autor original. El software de dominio público se puede utilizar, copiar, modificar y distribuir de forma gratuita sin necesidad de permisos o prerrogativas. El software se considera parte del patrimonio común porque está en dominio público. Puede ser utilizado como base para nuevos proyectos y aplicaciones. Esto fomenta el trabajo en equipo, la creatividad y la creación de soluciones de software innovadoras. Es importante tener en cuenta que el software de dominio público puede estar sujeto a ciertas limitaciones o restricciones en algunos países, por lo que es recomendable verificar las leyes y regulaciones locales antes de utilizar o distribuirlo.

En resumen, el software que se encuentra en el dominio público es aquel que no tiene derechos de autor y puede ser utilizado, modificado y distribuido por cualquier persona sin restricciones.

⁸ Rojas, B. S. Patentes de software, una tendencia estadounidense...

⁹ Ayuda Ley Protección Datos. (s.f.). Patentes de software

2.3 Propiedad intelectual y software

La propiedad intelectual y el software están estrechamente relacionados. El software es considerado una creación intelectual y, como tal, está protegido por leyes de propiedad intelectual en muchos países. Estas leyes otorgan derechos exclusivos al creador del software, permitiéndole controlar su reproducción, distribución y modificación.

El software se protege principalmente a través del derecho de autor, que otorga al creador o titular del software derechos exclusivos sobre su uso y distribución. Esto significa que cualquier persona o entidad que desee utilizar, copiar, distribuir o modificar el software necesita obtener el permiso del titular de los derechos de autor, a menos que exista una excepción o licencia que lo permita. Las licencias de software son contratos legales que establecen los términos y condiciones bajo los cuales se puede utilizar el software.

La propiedad intelectual es un concepto legal que se aplica a diversas formas de creaciones de la mente, como invenciones, obras literarias y artísticas, marcas comerciales y diseños industriales. En el contexto del software, la propiedad intelectual juega un papel crucial, ya que los programas informáticos son considerados creaciones intelectuales protegidas por derechos de autor.

Se trata de conseguir un equilibrio entre los derechos exclusivos y los límites y excepciones a los mismos para favorecer el acceso, es decir, se busca un equilibrio entre la propiedad y el acceso para promover la cultura.

En este aspecto hay un problema y es que, en la actualidad, el acceso supera a la propiedad. De este tema iremos tratando más adelante.

El futuro en cuanto a la propiedad intelectual y la protección de los derechos del autor pasa por el uso de modelos de acceso o streaming en vez de modelos de descarga.

La protección de la propiedad intelectual en el software es importante tanto para los creadores como para los usuarios. Para los creadores, la protección de sus derechos de propiedad intelectual les brinda incentivos para invertir tiempo y recursos en la creación de nuevos programas y soluciones innovadoras, además de la posibilidad de tomar acciones legales contra infractores y proteger su inversión y reputación. Para los usuarios, la protección de la propiedad intelectual garantiza que el software que utilizan sea legítimo y legalmente adquirido, lo que proporciona seguridad y confianza en su uso.

He de mencionar también que en ciertos casos el software puede protegerse mediante patentes las cuales cubren innovaciones técnicas y funcionales que son nuevas, no obvias y tienen aplicaciones industriales. Sin embargo, las leyes de patentes relacionadas con el software pueden variar según el país y pueden ser objeto de debate y controversia. Las patentes protegen invenciones técnicas novedosas y no obvias, por lo que solo ciertos aspectos del software pueden ser patentables.

Otro aspecto de la propiedad intelectual relacionado con el software es el secreto comercial. Algunas empresas optan por mantener en secreto su software y no revelar su código fuente. Esto les permite proteger su ventaja competitiva y mantener el control exclusivo sobre su software. Existe otro modo de proteger la propiedad intelectual que pueden ser relevantes para el software, se trata de las marcas registradas, que protegen los nombres o logotipos asociados con el software

Las licencias de software son acuerdos legales que establecen los términos y condiciones bajo los cuales se puede utilizar, copiar, distribuir y modificar el software. Estas licencias son herramientas importantes para proteger los derechos de autor y otros derechos de propiedad intelectual asociados al software.

Por lo tanto, la legislación relacionada con la propiedad intelectual y el software es un tema en constante evolución y adaptación a los avances tecnológicos y las necesidades de la sociedad.

2.3.1 Propiedad intelectual y derechos de autor en el software libre

¹⁰La propiedad industrial protege una variedad de invenciones y creaciones, y aunque no está completamente claro en cuanto a la protección de productos digitales, el software forma parte de las creaciones protegidas por la propiedad intelectual, más específicamente por el derecho de autor. A través de esta investigación, se ha recopilado información clara sobre la diversidad de licencias que actualmente rigen el software libre, así como qué tipo de licencia han adoptado los productos software utilizados en el desarrollo de software por los grupos de investigación involucrados. Existen actualmente diversas licencias bajo las cuales es posible proteger un producto software u otro tipo de creación, por lo que es importante conocer las características de las principales licencias para determinar cuál es la más adecuada en un caso específico. Aunque existen diversas licencias, la mayoría de los productos de software utilizan la Licencia Pública General, que garantiza que el producto, desde su origen hasta sus futuras versiones, ofrezca las cuatro libertades del software libre. Durante el proceso de ingeniería de software, es posible agilizar y optimizar las tareas utilizando herramientas apropiadas, tanto de carácter propietario como soluciones libres, que facilitan el desarrollo de las tareas asociadas. El software nació como software libre, pero ciertas circunstancias en un momento determinado lo convirtieron en un producto de software propietario, lo cual en cierta medida retrasó el avance tecnológico. A pesar de esto, el software libre sigue existiendo y cada día gana más fuerza y reconocimiento en el medio. Estas libertades en el desarrollo de software podrían complicar, desorganizar y no hacer seguro el proceso, por lo que es importante el licenciamiento en entornos libres de desarrollo.

2.4. Licencias de software

Como se mencionó en el punto anterior, ¹¹las licencias de software son contratos legales que establecen los términos y condiciones bajo los cuales se puede utilizar el software. ¹²Estas licencias definen los derechos y restricciones para los usuarios del software y pueden variar en cuanto a su nivel de apertura, permisos y obligaciones.

Las licencias de software variarán acorde con los ¹³diferentes tipos de software que ya fueron detallados con anterioridad. Algunas de estas licencias son:

¹⁰ Aldana, A. C. A., & Cuervo, M. C. (2009). Propiedad intelectual y derechos de autor en el software libre. Revista Virtual Universidad Católica del Norte, (28).

¹¹ Brocca, J. C., & Casamiquela, R. (2005). Las licencias de software. Revista Pilquen, (7), 0-0.

¹² Vega Alvarado, E., Toledo Molano, S., & Molina Vilchis, M. A. (2007). Licencias de Software: Antecedentes. Polibits, 35, 35-37.

¹³ Labrador, R. M. G. (2012). Tipos de licencias de software.

1. ¹⁴Licencia de software propietario: Un tipo de licencia conocida como licencia para software propietario, también conocida como licencia cerrada o comercial, restringe el uso, distribución, modificación y copia del software al mismo tiempo que otorga derechos exclusivos al propietario del software. A continuación se presentan algunas características de las licencias para software propietario:

1.-Limitaciones de uso: Estas licencias suelen establecer restricciones en el número de instalaciones, los dispositivos en los que se puede utilizar el software y la duración de la licencia.

2.-Protección mediante derechos de autor: Debido a que está protegido por derechos de autor, el software propietario no puede ser copiado, distribuido o modificado sin el permiso explícito del titular de los derechos.

3.-Licencias individuales: Cada cliente u organización que desee utilizar el software propietario debe obtener una licencia individual, generalmente mediante el pago de una tarifa de licencia.

4.- Actualizaciones y soporte: Las licencias para software propietario suelen incluir servicios de soporte técnico y actualizaciones periódicas del software para garantizar su funcionalidad y seguridad.

5.- Código fuente cerrado: En la mayoría de los casos, el código fuente del software propietario no está disponible para el público y solo el titular de los derechos tiene acceso a él.

Las licencias para software propietario permiten a los desarrolladores generar beneficios económicos a partir de su trabajo y mantener un control exclusivo sobre el software. Sin embargo, su uso puede implicar restricciones en la libertad de los usuarios para modificar o compartir el software.

2. ¹⁵Licencia de software de código abierto: Un tipo de licencia conocida como software de código abierto permite el uso, modificación y distribución gratuita y sin restricciones del software. Las licencias de software de código abierto tienen algunas de las siguientes características:

1.- Acceso al código fuente: Las licencias para software de código abierto requieren que los usuarios puedan ver, modificar y distribuir el código fuente del software.

2.- Capacidad de uso: El software se puede utilizar con cualquier propósito y en cualquier dispositivo en cualquier momento.

3.- Derecho a realizar cambios: El software puede ser modificado por los usuarios para satisfacer sus necesidades o solucionar errores.

4.- Derecho de distribución: Los clientes pueden distribuir el software a otras personas, ya sea de forma gratuita o mediante un pago, siempre y cuando cumplan con las especificaciones de la licencia.

5.- Transparencia: Al permitir a los usuarios acceder al código fuente y comprender cómo funciona el software, las licencias de software de código abierto fomentan la transparencia.

6.- Colaboración: Las licencias para software de código abierto permiten que varias personas contribuyan a la mejora y desarrollo del software, fomentando la colaboración entre desarrolladores y usuarios.

¹⁴ Tecnoadmin. (2019, 26 septiembre). Software Propietario: ¿Qué es? Características y Ejemplos. TecnoMagazine.

¹⁵ Gomez Diaz, T. (2015). Software libre, software de código abierto, licencias. Donde se propone un procedimiento de distribución de software y datos de investigación. HAL Id: hal-01261064.

3. ¹⁶Licencia de software libre: Un tipo de licencia conocida como licencia de software libre permite a los usuarios utilizar, modificar y distribuir el software sin costo alguno. A continuación se presentan algunas características de las licencias de software libre:

1.- Capacidad de uso: El software se puede utilizar con libertad para cualquier propósito y en cualquier dispositivo.

2.- Acceso al código fuente: La disponibilidad del código fuente del software para que los usuarios lo vean, modifiquen y distribuyan es un requisito de las licencias de software libre.

3.- Derecho de modificar: Los clientes tienen el derecho de modificar el software para adaptarlo a sus necesidades o corregir errores.

4.- Derecho de distribución: Los clientes pueden distribuir el software a otras personas, ya sea de forma gratuita o a cambio de un pago, siempre y cuando cumplan con los términos de la licencia.

5.- Transparencia: Las licencias de software libre fomentan la transparencia al permitir que los usuarios accedan al código fuente y comprendan cómo funciona el software.

6.- Colaboración: Las licencias de software libre fomentan la colaboración entre los desarrolladores y los usuarios, permitiendo que varias personas contribuyan al desarrollo y mejora del software.

Algunas licencias de software libre populares incluyen la Licencia Pública General de GNU (GPL), la Licencia MIT, la Licencia Apache y la Licencia de Documentación Gratuita de GNU (GFDL). Las licencias de software libre garantizan la libertad del usuario y fomentan la colaboración y el acceso abierto al código fuente.

4. ¹⁷Licencia de software de dominio público: Una licencia para software de dominio público es un tipo de licencia que permite que el software esté libre y abiertamente disponible para el público en general. Algunas características de las licencias para software de dominio público son:

1.- Sin limitaciones: El software que se encuentra en el dominio público puede ser utilizado, modificado y distribuido sin restricciones. No requiere permisos adicionales para ser utilizado libremente por cualquier persona.

2.- Renuncia de derechos de autor: El software ya no está protegido por derechos de autor porque el propietario de los derechos renuncia a ellos y permite que entre en el dominio público.

3.- Sin limitaciones de propiedad intelectual: El software de dominio público puede ser utilizado, modificado y distribuido prácticamente sin limitaciones de propiedad intelectual, lo que brinda mayor libertad a los usuarios.

4.- Herencia común: El software que se considera parte del patrimonio común puede ser utilizado por cualquier persona para desarrollar nuevos proyectos y aplicaciones.

Es importante tener en cuenta que las licencias para software de dominio público pueden variar de un país a otro; por lo tanto, se recomienda verificar las regulaciones locales antes de utilizar o distribuir el software.

¹⁶ González Barahona, J., Seoane Pascual, J., & Robles, G. (2003). *Introducción al software libre*. Barcelona: Fundació per a la Universitat Oberta de Catalunya, 2003..

¹⁷ NASA. (s.f.). What Is an Evaluation License, and Is It Right for You?

5. ¹⁸Licencia de software de evaluación: Una licencia de software de evaluación es un tipo de licencia que permite a los usuarios evaluar y probar la funcionalidad de un producto de software durante un período de tiempo limitado. Las licencias de software de evaluación tienen las siguientes características:

1.- Duración limitada: Las licencias de software de evaluación tienen un período de tiempo preestablecido durante el cual se puede utilizar el software con fines de evaluación. Una vez que el período de evaluación ha expirado, el software generalmente se vuelve inutilizable o limitado en su funcionalidad.

2.- Uso restringido: Las licencias de software de evaluación imponen restricciones en el uso del software, como limitar el número de instalaciones o usuarios o prohibir el uso comercial.

3.- Sin distribución ni modificación: La mayoría de las licencias de software de evaluación no permiten modificar o distribuir el software. El software está destinado únicamente para fines de evaluación y no debe ser modificado ni compartido.

4.- Sin garantía ni soporte: El software de evaluación se proporciona generalmente "tal cual" sin garantía o soporte técnico por parte del proveedor del software. Los usuarios son responsables de evaluar el software por sí mismos y bajo su propio riesgo.

5.- Conversión a una licencia completa: En algunos casos, los usuarios tienen la opción de convertir el software de evaluación en una licencia completa mediante la compra de una versión comercial del software.

Por tanto, es importante recalcar que antes de utilizar un cierto software se deben leer y comprender los términos de la licencia de dicho software ya que esta determinará lo que se puede hacer con el software y los derechos que se tienen sobre el mismo.

3. Protección jurídica del software

3.1. Marco legal del software en la Unión Europea

El marco legal de la Unión Europea para el software se basa en una variedad de directivas y regulaciones que tienen como objetivo proteger los derechos de propiedad intelectual, promover la competencia justa y garantizar la libre circulación del software dentro del mercado único. El marco legal de la Unión Europea para el software incluye los siguientes aspectos clave:

Ley de derechos de autor: En la Unión Europea, el software se considera una obra protegida por derechos de autor. Esto significa que está sujeto a la Directiva de Derechos de Autor de la Unión Europea y a las leyes nacionales de derechos de autor de los Estados miembros.

Licencias de software: Las licencias de software son contratos legales que establecen los términos y condiciones para el uso del software. Las licencias de software son válidas y exigibles, y la Unión Europea fomenta el uso de licencias que protejan los derechos de los titulares de derechos de autor y promuevan la competencia.

Competencia: El software está sujeto a regulaciones de competencia en la Unión Europea para prevenir prácticas anticompetitivas como el abuso de posición dominante y los acuerdos

¹⁸ Gobierno de Canarias. (s.f.). Licencia de dominio público.

anticompetitivos. Estas prácticas pueden ser investigadas y sancionadas por la Comisión Europea.

Seguridad de datos: El software que maneja datos personales está sujeto a la legislación de protección de datos de la Unión Europea, como el Reglamento General de Protección de Datos (RGPD). Esto implica garantizar la privacidad y seguridad de los datos personales procesados por el software.

Normas e interoperabilidad: La Unión Europea promueve la adopción de normas abiertas e interoperabilidad entre sistemas y aplicaciones de software para facilitar la competencia y la integración de soluciones tecnológicas.

Es importante tener en cuenta que el marco legal para el software puede variar ligeramente entre los Estados miembros de la Unión Europea, ya que cada país puede tener regulaciones nacionales adicionales o específicas. Por lo tanto, se recomienda consultar las leyes y pautas específicas de cada país de la Unión Europea para obtener información detallada sobre el marco legal para el software en ese contexto.

El marco legal del software en la Unión Europea se basa en varias leyes y regulaciones que abordan diferentes aspectos relacionados con los derechos de autor, la protección de datos y la competencia. A continuación, se mencionan las principales normativas relevantes:

1. ¹⁹Directiva sobre el Derecho de Autor en el Mercado Único (2019/790): tiene como objetivo modernizar las leyes de derechos de autor y armonizarlas dentro del mercado único europeo. La directiva aborda diversos aspectos del derecho de autor en la era digital e introduce nuevas disposiciones para adaptar las normas de derechos de autor al entorno digital. Algunas disposiciones clave de la directiva incluyen:
Plataformas en línea y responsabilidad por derechos de autor: La directiva establece nuevas obligaciones para las plataformas en línea, como las plataformas de intercambio de contenido y los sitios de redes sociales, para que tomen medidas para prevenir la infracción de derechos de autor. Las plataformas pueden ser consideradas responsables por el contenido no autorizado cargado por sus usuarios.
Uso de contenido protegido por derechos de autor por parte de los editores de noticias: La directiva otorga a los editores de noticias el derecho de negociar y obtener una compensación justa por el uso en línea de sus artículos de noticias por parte de plataformas en línea o agregadores de noticias.
Minería de texto y datos: La directiva establece una excepción al derecho de autor para las actividades de minería de texto y datos realizadas con fines de investigación científica. Los investigadores pueden utilizar obras protegidas por derechos de autor para minería y análisis sin solicitar permiso a los titulares de derechos.
Derechos ampliados para autores e intérpretes: La directiva fortalece la posición de los autores y los intérpretes al otorgarles derechos adicionales, incluido el derecho a recibir una remuneración justa y proporcionada por la explotación de sus obras.
Acceso en línea a obras fuera de comercio: La directiva establece mecanismos para facilitar la digitalización y disponibilidad en línea de obras fuera de comercio, haciéndolas accesibles al público mientras se garantiza una remuneración justa para los titulares de derechos.

¹⁹ Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre el derecho de autor y los derechos afines en el mercado único digital y por la que se modifica la Directiva 96/9/CE y la Directiva 2001/29/CE. (2019). Diario Oficial de la Unión Europea, L130, 1-63.

Contenido generado por usuarios: La directiva aclara el estatus legal del contenido generado por usuarios, estableciendo que el uso de contenido protegido por derechos de autor en memes, parodias y otras formas de contenido generado por usuarios está permitido siempre que se encuentre dentro del ámbito de la cita y no infrinja los derechos de los creadores de contenido original.

La implementación de la directiva en las leyes nacionales de los Estados miembros de la Unión Europea está en curso y las disposiciones específicas pueden variar entre países.

2. ²⁰Reglamento General de Protección de Datos (RGPD): El objetivo del Reglamento General de Protección de Datos (GDPR) de la Unión Europea es salvaguardar la privacidad y los datos personales de los individuos dentro de la UE. El Reglamento General de Protección de Datos (GDPR) reemplaza la Directiva de Protección de Datos anterior, establece regulaciones más estrictas y amplía los derechos de los individuos.

Las disposiciones más importantes del GDPR incluyen:

Aplicación territorial y alcance: Cualquier empresa que maneje información personal de residentes de la UE está sujeta al GDPR, sin importar dónde esté ubicada.

Justificación legítima para el tratamiento: Al procesar datos personales, las organizaciones deben tener una justificación legal, como obtener consentimiento, cumplir con una obligación legal, cumplir con un contrato, proteger intereses vitales, llevar a cabo una tarea de interés público o tener intereses legítimos.

Consentimiento: El consentimiento para el procesamiento de datos personales debe ser inequívoco, específico, informado y otorgado libremente. El consentimiento puede ser revocado en cualquier momento por cualquier persona.

Derechos individuales: Se otorgan a los individuos una serie de derechos en virtud del GDPR, incluido el derecho de acceso, rectificación y supresión de sus datos personales (el "derecho al olvido"), limitar el procesamiento, permitir la portabilidad de datos y oponerse al procesamiento.

Seguridad de datos por defecto y por diseño: Para garantizar que los principios de protección de datos estén incorporados en sus sistemas y procedimientos desde el principio, las organizaciones deben implementar medidas técnicas y organizativas.

Violaciones de seguridad: En caso de una violación de datos personales que represente una amenaza para los derechos y libertades de las personas, las empresas deben notificar a la autoridad de supervisión relevante y a los individuos afectados dentro de un plazo determinado.

Evaluaciones de impacto en la protección de datos: Antes de participar en actividades de procesamiento de datos de alto riesgo, las organizaciones deben evaluar el impacto potencial en la privacidad de las personas y tomar medidas para reducir cualquier riesgo.

DPO: Oficial de Protección de Datos (DPO). Un Oficial de Protección de Datos supervisa las actividades de protección de datos y sirve como punto de contacto para los individuos y las autoridades de supervisión en algunas organizaciones.

Transferencias de datos transfronterizas: El GDPR proporciona mecanismos para la transferencia legal de datos personales fuera de la UE, asegurando que los datos de los individuos estén adecuadamente protegidos.

²⁰ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (2016). Diario Oficial de la Unión Europea, 59, 1-88.

Cumplimiento y sanciones: El incumplimiento del GDPR puede resultar en multas significativas, de hasta 20 millones de euros o el 4% de los ingresos anuales globales de la empresa, según corresponda.

El GDPR tiene como objetivo armonizar las leyes de protección de datos dentro de la UE y mejorar el control de los individuos sobre sus datos personales. Impone importantes obligaciones a las organizaciones y establece un marco para el procesamiento seguro y responsable de datos personales.

3. ²¹Directiva de Licencia Pública General (GPL): hace referencia a la "GNU General Public License" (GPL), que es una licencia de software de código abierto ampliamente utilizada. La GPL establece los términos y condiciones para el uso, modificación y distribución del software libre. Algunas características importantes de la Licencia Pública General incluyen:

Derechos de uso y distribución: La GPL permite a los usuarios utilizar, copiar, modificar y distribuir el software de acuerdo con los términos de la licencia.

Código fuente disponible: La GPL requiere que el código fuente del software esté disponible para los usuarios, lo que les permite ver y modificar el software según sea necesario.

Obras y derivados: Si se crea una obra derivada a partir del software con licencia GPL, también debe estar sujeta a los términos de la GPL y distribuirse como software libre.

Copyleft: La GPL utiliza el concepto de "copyleft", lo que significa que cualquier obra derivada del software debe mantener los mismos derechos de uso, modificación y distribución.

Compatibilidad: La GPL es compatible con otras licencias de software de código abierto y permite la combinación de software bajo diferentes licencias, siempre y cuando se cumplan los requisitos de la GPL.

En la comunidad de software libre, la Licencia Pública General es una licencia popular que se ha utilizado en muchos proyectos de software significativos, como el kernel de Linux.

4. ²²Directiva sobre Comercio Electrónico (2000/31/CE): La directiva incluye los siguientes puntos clave:

Legalización de actividades en línea: La directiva garantiza que los contratos electrónicos y las transacciones en línea tengan la misma validez legal que los contratos tradicionales en papel.

Requisitos de información para proveedores de servicios en línea: Los proveedores de servicios en línea deben proporcionar cierta información a los consumidores, como sus datos de contacto, información de registro y cualquier licencia o membresía profesional relevante.

Limitación de responsabilidad para intermediarios: La directiva establece un régimen de responsabilidad limitada para proveedores de servicios de Internet, proveedores de alojamiento y otros intermediarios, protegiéndolos de la responsabilidad por el contenido transmitido o almacenado por sus usuarios, siempre y cuando actúen de manera oportuna para eliminar o deshabilitar el acceso al contenido ilegal.

²¹ Free Software Foundation. (2007). GNU General Public License version 3.0.

²² Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. (2000). Diario Oficial de la Unión Europea, L 178, 1-16.

Comunicaciones comerciales no solicitadas: La directiva prohíbe el envío de comunicaciones comerciales no solicitadas, como correos electrónicos no deseados, sin el consentimiento previo del destinatario.

Protección al consumidor: La directiva establece el derecho a recibir información clara y transparente, el derecho a desistir de una compra dentro de un período determinado y la prohibición de prácticas comerciales desleales para proteger a los consumidores durante las transacciones en línea.

Principio del país de origen: La directiva promueve el principio de que los proveedores de servicios en línea deben cumplir con las leyes y regulaciones de su país de origen en lugar de las leyes de cada Estado miembro de la UE donde se accede a sus servicios.

La Directiva sobre Comercio Electrónico de la UE armoniza las regulaciones, facilitando las transacciones electrónicas transfronterizas y brindando certeza jurídica a los consumidores y las empresas en línea.

5. ²³Ley de Competencia de la UE: La Regulación de Competencia de la UE se refiere a un conjunto de normas y regulaciones destinadas a promover la competencia justa y proteger los derechos de los consumidores dentro del mercado único de la Unión Europea. Los aspectos más importantes de la Ley de Competencia de la UE son los siguientes:

Prohibición de prácticas anticompetitivas: La Ley de Competencia prohíbe acuerdos y prácticas que restrinjan la competencia, como los cárteles, abusos de posición dominante y fusiones que puedan obstaculizar la competencia efectiva.

6. Control de fusiones y adquisiciones: La Ley de Competencia establece un sistema para controlar las fusiones y adquisiciones con el fin de prevenir concentraciones excesivas de poder económico que puedan perjudicar la competencia en el mercado.

Ayudas estatales: La Ley de Competencia regula las ayudas estatales que los gobiernos de los Estados miembros pueden otorgar a las empresas, asegurando que no distorsionen la competencia en el mercado.

Protección al consumidor: La Ley de Competencia busca proteger los derechos de los consumidores promoviendo la transparencia en la publicidad, combatiendo prácticas comerciales desleales y garantizando la libre elección y competencia en beneficio de los consumidores.

Investigaciones y sanciones: La Comisión Europea, a través de la Dirección General de Competencia, tiene la autoridad para investigar y tomar medidas en caso de infracciones de la Ley de Competencia. Las sanciones por incumplimiento pueden incluir multas significativas y otras medidas correctivas.

La Ley de Competencia de la UE tiene como objetivo fomentar la innovación, eficiencia y beneficios para los consumidores en toda la Unión Europea al garantizar un mercado único justo y competitivo.

Es importante destacar que estas son solo algunas de las leyes y regulaciones relevantes en la Unión Europea. El marco legal puede variar según los países miembros y existen otras regulaciones específicas relacionadas con la protección de datos, la seguridad cibernética y la propiedad intelectual que también pueden ser aplicables al software.

²³ Comisión Europea. (s.f.). Antitrust: European Commission.

3.2. Marco legal del software en España

La ley del software en España se basa en diversas leyes y regulaciones que abordan aspectos como el derecho de autor, la protección de datos, la competencia y la responsabilidad civil. A continuación, se presentan las regulaciones más significativas:

1. ²⁴Ley de Propiedad Intelectual (Ley 1/1996): conocida como "Ley de Propiedad Intelectual", administra la protección y regulación de los derechos de propiedad intelectual en diversas obras creativas. A continuación se presentan aspectos importantes de la Ley de Propiedad Intelectual:

Protección del derecho de autor: La ley otorga a los autores y creadores la plena propiedad de sus obras literarias, artísticas y científicas, como software, música y películas. Los derechos de reproducción, distribución, comunicación pública y modificación de las obras están cubiertos por estos derechos.

Derechos morales: Los autores tienen el derecho de preservar la integridad de sus obras y ser reconocidos como sus creadores. Los derechos morales no pueden ser transferidos y son perpetuos.

Derechos económicos: Los autores tienen el derecho de obtener beneficios económicos de sus obras y recibir una compensación justa por su uso. Los derechos económicos pueden ser licenciados o cedidos a terceros.

Otros derechos: Los intérpretes, productores de fonogramas y organizaciones de radiodifusión tienen derechos específicos relacionados con sus actuaciones, grabaciones y emisiones.

Duración de la protección: La protección del derecho de autor generalmente dura toda la vida del autor más 70 años post mortem. En el caso de obras conjuntas, la duración se determina por la vida del último autor superviviente.

Excepciones y limitaciones: La ley establece ciertas excepciones y limitaciones al derecho de autor, como para fines educativos o de investigación, copia privada y parodia.

Entidades de gestión colectiva: Las entidades de gestión colectiva son responsables de administrar y hacer cumplir los derechos de los autores y otros titulares de derechos, incluida la recaudación y distribución de regalías.

Cumplimiento y sanciones: Para las infracciones de los derechos de propiedad intelectual, la ley prevé remedios y sanciones, como medidas cautelares, indemnizaciones, multas y sanciones penales.

La Ley de Propiedad Intelectual en España tiene como objetivo promover la creatividad, proteger los derechos de los autores y creadores, y fomentar el desarrollo de obras intelectuales y culturales.

2. ²⁵Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE): es una ley española que regula el comercio electrónico y los servicios de la sociedad

²⁴ Ley 1/1996, de 12 de abril, de Propiedad Intelectual. (1996). Boletín Oficial del Estado, 97, 1-39.

²⁵ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico. (2002). Boletín Oficial del Estado, 166, 28470-28503.

de la información en España. Algunos aspectos importantes de la LSSI-CE son los siguientes:

Ámbito de aplicación: La ley se aplica a cualquier actividad económica realizada por vía electrónica, así como a los servicios de la sociedad de la información, incluyendo el comercio electrónico, la publicidad online, los servicios en línea, y la prestación de información a través de medios electrónicos.

Información obligatoria: Los prestadores de servicios deben facilitar a los usuarios información clara, completa y fácilmente accesible sobre su identidad, ubicación, contacto, y datos registrales, así como sobre las características esenciales de los productos o servicios ofrecidos.

Comunicaciones comerciales: La LSSI-CE establece requisitos para las comunicaciones comerciales realizadas por vía electrónica, como el envío de correos electrónicos promocionales o newsletters, incluyendo la obligación de obtener el consentimiento previo del destinatario.

Responsabilidad de los intermediarios: La ley establece que los prestadores de servicios de la sociedad de la información no son responsables de los contenidos generados por terceros, pero deben actuar de manera diligente para retirar o bloquear el acceso a contenidos ilícitos o lesivos una vez tengan conocimiento de ellos.

Protección de datos personales: La LSSI-CE establece las obligaciones que deben cumplir los prestadores de servicios en materia de protección de datos personales, garantizando el cumplimiento de la normativa de protección de datos vigente.

Sanciones: En caso de incumplimiento de la ley, se establecen sanciones que pueden variar en función de la gravedad de la infracción, incluyendo multas económicas y otras medidas correctivas.

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico tiene como objetivo fomentar la confianza en el comercio electrónico y garantizar la protección de los derechos de los usuarios en el entorno digital

3. ²⁶Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD): es una ley española que establece las normas y regulaciones para la protección de datos personales y los derechos digitales en España. Algunos aspectos importantes de la LOPDGDD son los siguientes:

Derechos de los interesados: La ley reconoce y garantiza los derechos de las personas sobre sus datos personales, incluyendo el derecho de acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad de sus datos.

Consentimiento: Se establecen requisitos específicos para obtener el consentimiento válido de los interesados para el tratamiento de sus datos personales, asegurando que sea libre, específico, informado e inequívoco.

Responsabilidad y accountability: La ley establece la responsabilidad de los responsables del tratamiento de datos (empresas, organizaciones, etc.) y les obliga a implementar

²⁶ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. (2018). Boletín Oficial del Estado, 294, 119954-120076.

medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos y el cumplimiento de la normativa.

Delegado de Protección de Datos (DPD): Se regula la figura del Delegado de Protección de Datos, quien será responsable de supervisar y asesorar sobre el cumplimiento de la normativa de protección de datos en las organizaciones.

Transferencias internacionales: Se establecen las condiciones y requisitos para realizar transferencias internacionales de datos personales a países fuera de la Unión Europea, garantizando un nivel adecuado de protección.

Protección de los derechos digitales: La ley también garantiza los derechos de los ciudadanos en el entorno digital, incluyendo la protección de la intimidad, el derecho al olvido, la neutralidad de la red, la seguridad digital y el acceso a la información.

Sanciones y control: Se establecen sanciones económicas y otras medidas correctivas para aquellos que no cumplan con la normativa de protección de datos. Además, se establece la Agencia Española de Protección de Datos como la autoridad de control y supervisión en esta materia.

4. ²⁷Ley de Competencia, Ley 15/2007: Esta regulación dirige la competencia y la protección de la competencia en España y puede aplicarse a casos relacionados con el software. La ley prohíbe los acuerdos y prácticas que limitan la competencia, como los cárteles, los abusos de posición dominante y las prácticas que restringen la competencia.

Control de concentraciones empresariales: Se establece un sistema de control de fusiones y adquisiciones para prevenir concentraciones excesivas que puedan perjudicar la competencia en el mercado.

Control de ayudas estatales: La ley regula la asistencia económica que los organismos públicos pueden otorgar a las empresas para evitar distorsiones en la competencia del mercado.

Promoción de la competencia: La ley fomenta la competencia efectiva en el mercado al fomentar la entrada de nuevas empresas, prevenir prácticas restrictivas y fomentar la innovación.

Sanciones e investigación: La Comisión Nacional de los Mercados y la Competencia (CNMC) tiene la autoridad para investigar y sancionar conductas anticompetitivas, imponiendo multas y adoptando medidas correctivas.

Colaboración entre países: Con el fin de garantizar la competencia en el mercado global, la ley establece la cooperación y coordinación con las autoridades de competencia de otros países y organizaciones internacionales.

En España, la Ley de Competencia tiene como objetivo promover la eficiencia económica, salvaguardar los intereses de los consumidores y garantizar una competencia justa en el mercado.

²⁷ Ley 15/2007, de 3 de julio, de Defensa de la Competencia. (2007). Boletín Oficial del Estado, 159, 28143-28170.

5. ²⁸Reglamento de Servicios de la Sociedad de la Información (LSSI) (Real Decreto 1/2007): tiene como objetivo regular la prestación de servicios de la sociedad de la información dentro de España. Las características más importantes del LSSI son las siguientes:

Servicios de la sociedad de la información: El reglamento se aplica a los servicios prestados electrónicamente, incluyendo el comercio en línea, los contratos electrónicos y la provisión de contenido o información a través de medios digitales.

Requisitos de información: Los proveedores de servicios deben proporcionar cierta información a los usuarios, como su identificación, datos de contacto, información de registro y cualquier licencia o membresía profesional relevante.

Contratos electrónicos: El reglamento establece normas para la validez y eficacia de los contratos electrónicos, incluyendo el uso de firmas electrónicas y la obligación de proporcionar términos contractuales claros y accesibles.

Comunicaciones comerciales: El LSSI regula el envío de comunicaciones comerciales por medios electrónicos, requiriendo el consentimiento previo de los destinatarios y proporcionando mecanismos para optar por no recibirlas y darse de baja.

Responsabilidad de los proveedores de servicios: El reglamento establece un procedimiento de aviso y retirada para el contenido ilegal o perjudicial y describe la responsabilidad de los proveedores de servicios por el contenido que alojan o transmiten.

Protección de datos: El LSSI complementa las regulaciones de protección de datos al establecer requisitos para el tratamiento de datos personales en la prestación de servicios de la sociedad de la información.

Cumplimiento y sanciones: El incumplimiento del LSSI puede conllevar sanciones, incluyendo multas y la suspensión o cierre de las actividades del proveedor de servicios.

El Reglamento de los Servicios de la Sociedad de la Información en España, como se establece en el LSSI, tiene como objetivo garantizar la transparencia, la seguridad y la protección del consumidor en el entorno digital.

Deberemos también tener en cuenta que estas son solo algunas de las regulaciones relevantes en España, y la estructura legal del software puede variar según los contextos específicos y el uso del software.

3.3. Protección de los derechos de autor en el software

En el ámbito legal, proteger los derechos de autor en el software es un aspecto fundamental. Los derechos de autor se aplican a las obras originales de autoría, y el software puede considerarse una obra protegida por derechos de autor.

²⁸ Real Decreto 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. (2007). Boletín Oficial del Estado, 295, 52887-52918.

A continuación se destacan algunos aspectos clave relacionados con la protección de los derechos de autor en el software:

Copyright del código fuente: El código fuente de un programa de software está protegido automáticamente por los derechos de autor en la mayoría de los países. Esto significa que el autor tiene el derecho exclusivo de copiar, distribuir y modificar el código fuente.

Licencias de software: Las licencias de software son acuerdos legales que permiten a los usuarios utilizar el software de acuerdo con los términos establecidos por el titular de los derechos de autor. Las licencias pueden imponer restricciones sobre la copia, distribución y modificación del software.

Registro de derechos de autor: Aunque el registro de derechos de autor no es obligatorio para obtener protección, en algunos países es recomendable registrar el software para tener pruebas de su autoría en caso de disputas legales.

Protección de algoritmos y funcionalidades: En algunos casos, los algoritmos o las funcionalidades específicas de un software pueden estar protegidos por derechos de autor si se consideran una expresión original y creativa.

Protección de interfaces y apariencia gráfica: Además del código fuente, los elementos visuales de un software, como la interfaz de usuario y la apariencia gráfica, también pueden recibir protección de derechos de autor.

En la mayoría de los casos, el titular de los derechos de autor del software tiene derechos exclusivos sobre la reproducción, distribución, comunicación pública y transformación de la obra. Esto significa que nadie puede realizar estas acciones sin el permiso del titular, a menos que exista una excepción o limitación legal.

²⁹Se deben tomar las siguientes medidas para salvaguardar los derechos de autor en el software:

1. **Registro de derechos de autor:** Es recomendable registrar el software ante la entidad competente de propiedad intelectual en tu país. El registro puede proporcionar evidencia adicional de tu titularidad sobre la obra en caso de disputas legales.
2. **Patentes y marcas:** Además de los derechos de autor, puede ser necesario obtener protección adicional mediante marcas registradas y patentes, especialmente si el software tiene características distintivas o novedosas.
3. **Vigilancia y cumplimiento:** Es fundamental estar atento al uso del software y tomar medidas legales para detener cualquier uso ilegal o violación. Esto podría implicar enviar avisos de cesación y desistimiento, realizar reclamaciones o tomar otras acciones legales necesarias.
4. **Infracción de derechos de autor:** La reproducción no autorizada, distribución o modificación del software protegido por derechos de autor sin el permiso del titular constituye una infracción de derechos de autor y puede dar lugar a acciones legales, como demandas por daños y perjuicios, así como a la adopción de medidas cautelares para detener la infracción.

Deberemos en cuenta también que las leyes de derechos de autor pueden variar en cada país.

²⁹ Blawie, J. R., & Klancnik, R. P. (2014). Copyright Protection of Computer Software. *Journal of the Copyright Society of the U.S.A.*, 61(4).

3.4. Protección de las patentes de software

La protección de las patentes de software es un tema complejo y controvertido en muchos países. Las patentes de software son derechos exclusivos otorgados a los inventores o titulares de una invención de software para proteger su creación y permitirles controlar su uso y comercialización. Sin embargo, la patentabilidad de software y los límites de protección varían según la legislación de cada país.

En algunos países, como Estados Unidos y Japón, es posible obtener patentes de software, siempre y cuando se cumplan ciertos requisitos establecidos por las leyes de patentes. Estos requisitos generalmente incluyen la demostración de una invención técnica, la novedad, la actividad inventiva y la aplicabilidad industrial del software. Sin embargo, incluso en estos países, existen restricciones y excepciones específicas para evitar la protección excesiva de ideas abstractas o métodos comerciales.

En otros países, como los países de la Unión Europea, la situación es diferente. La legislación europea de patentes excluye expresamente la patentabilidad de programas de ordenador "como tales", lo que significa que los programas de ordenador como tal no son patentables. Sin embargo, se permite la protección de invenciones que tienen una contribución y un efecto técnicos, aunque estén implementadas mediante software. Esto significa que se pueden obtener patentes para invenciones que resuelven un problema técnico utilizando software, pero no para software en sí.

Es importante tener en cuenta que la protección de las patentes de software varía según el país y su legislación específica. Además, la discusión sobre la patentabilidad del software y su impacto en la innovación y la competencia continúa en muchos foros y tribunales. Algunos argumentan que la patentabilidad del software promueve la innovación y la protección de la propiedad intelectual, mientras que otros argumentan que puede obstaculizar la creatividad, dificultar la interoperabilidad y permitir el monopolio de ideas abstractas.

En conclusión, la protección de las patentes de software es un tema complejo y su disponibilidad y alcance varían según el país.

Requisitos para la patentabilidad de software:

Los requisitos para obtener una patente de software suelen ser más estrictos que para otros campos tecnológicos. Algunos de los requisitos comunes incluyen:

Novedad: La invención debe ser nueva y no haber sido divulgada públicamente antes de la solicitud de patente.

Actividad inventiva: La invención debe implicar un avance técnico o una solución no obvia para un problema técnico.

Aplicación industrial: La invención debe ser susceptible de ser utilizada en una actividad industrial o comercial.

Áreas patentables en el software:

Las patentes de software pueden abarcar diferentes áreas, como algoritmos, métodos de procesamiento de datos, interfaces de usuario, tecnologías de comunicación, software

embebido en dispositivos y mucho más. Sin embargo, las ideas abstractas o conceptos matemáticos puros generalmente no son considerados patentables

Retos y debates:

La patentabilidad de software ha generado debates y desafíos legales debido a preocupaciones sobre la expansión excesiva de las patentes y su impacto en la innovación y la competencia. Algunos argumentan que las patentes de software pueden obstaculizar el desarrollo y la colaboración en la industria del software.

Limitaciones y excepciones:

Algunas jurisdicciones tienen limitaciones y excepciones específicas para la patentabilidad del software. Por ejemplo, las ideas abstractas, los algoritmos matemáticos y los métodos comerciales pueden no ser considerados patentables en algunas jurisdicciones.

Protección alternativa para el software:

Además de la protección mediante patentes, los derechos de autor y los secretos comerciales también pueden brindar protección para el software. El derecho de autor protege la expresión original del software, mientras que los secretos comerciales pueden proteger información confidencial o métodos comerciales utilizados en el desarrollo del software.

3.5. Protección de las marcas en el software

La protección de marcas en el software se refiere a los procedimientos legales utilizados para proteger y registrar marcas comerciales asociadas con productos o servicios de software. Un nombre de marca es un signo distintivo que identifica y diferencia los productos o servicios de una empresa de los de otras empresas.

Nombres comerciales, logotipos, eslóganes y otros elementos distintivos que identifican y promueven un producto o servicio de software en el mercado son ejemplos de marcas comerciales en la industria del software. La protección de los nombres comerciales en el software tiene como objetivo evitar la confusión o el uso no autorizado de nombres comerciales similares por parte de terceros.

Para proteger una marca comercial en el software, se puede presentar una solicitud de registro de marca ante la oficina de marcas comerciales correspondiente en el país donde se busca la protección. La solicitud y el cumplimiento de los requisitos legales, como la distintividad y la no confusión con marcas comerciales existentes, son necesarios para el registro de la marca.

Protección de las marcas en el software:

En el contexto del software, las marcas se utilizan para identificar los productos o servicios relacionados con el software, como nombres de programas, logotipos de aplicaciones o servicios en línea. La protección de las marcas en el software se puede lograr mediante el registro de la marca ante la oficina de marcas correspondiente.

Registro de marcas:

El registro de una marca en el ámbito del software proporciona al titular de la marca derechos exclusivos sobre su uso en el mercado. Permite proteger la identidad y reputación de una empresa y evitar confusiones con otras marcas similares.

Una vez registrada, la marca comercial en el software otorga al titular derechos exclusivos para utilizarla en relación con los productos o servicios específicos para los cuales se registró. Esto permite al titular proteger su identidad comercial y emprender acciones legales contra aquellos que utilicen la marca sin autorización o la infrinjan.

Uso de marcas en el software:

Es importante utilizar marcas de manera adecuada y consistente en el software. Esto implica incluir avisos de marca registrada (como el símbolo ®) y mantener la integridad de la marca en todas las comunicaciones y presentaciones del software.

Vigilancia y defensa de marcas:

Una vez registrada, es esencial vigilar y defender activamente la marca contra cualquier infracción o uso indebido. Esto implica monitorear el mercado y tomar acciones legales si se detecta alguna violación de los derechos de marca.

4. Piratería y violación de derechos de propiedad intelectual

4.1. Concepto de piratería informática

El acto de obtener acceso no autorizado a sistemas informáticos, redes, dispositivos electrónicos o servicios en línea con la intención de robar, dañar, modificar o comprometer la información contenida en ellos se conoce como piratería informática, también conocida como hacking o ciberdelito. Los hackers, que también son conocidos como piratas informáticos, utilizan una variedad de métodos y herramientas para cometer actos ilegales.

La piratería informática puede implicar aprovechar vulnerabilidades en el software, los sistemas operativos o las aplicaciones, así como utilizar técnicas de ingeniería social para engañar a los usuarios y obtener acceso a sus cuentas o información confidencial. Los hackers tienen la capacidad de ingresar a sistemas para robar información personal, financiera o empresarial, acceder a secretos comerciales, interrumpir el funcionamiento normal de los servicios en línea o incluso llevar a cabo actividades maliciosas como sabotaje o robo de identidad.

La piratería informática puede tomar también un sentido favorable en lo que respecta a la seguridad. El hacking ético tiene como objetivo encontrar y solucionar fallos de seguridad, y se lleva a cabo con el permiso del propietario del sistema o la red. Las empresas suelen contratar hackers éticos para probar la seguridad de sus sistemas.

La piratería informática es ilegal y puede tener graves repercusiones tanto para las personas afectadas como para las organizaciones. Los expertos en ciberseguridad colaboran con los gobiernos y las fuerzas del orden para combatir y prevenir estos delitos, y se establecen leyes y regulaciones para sancionar a los infractores.

4.2. Tipos de piratería

La piratería informática puede adoptar muchas formas, algunas de las cuales son las siguientes:

1. Ataques de phishing: Los ataques de phishing son intentos deliberados de engañar a las personas para que entreguen información privada como contraseñas, números de tarjetas de crédito u otra información sensible. Estos ataques se llevan a cabo a menudo mediante llamadas telefónicas, mensajes de texto, correos electrónicos o sitios web falsos que suplantan a organizaciones de confianza. Los atacantes utilizan estrategias de ingeniería social para elaborar comunicaciones persuasivas y lograr que los usuarios divulguen su información personal. Los correos electrónicos que animan a los usuarios a actualizar su información o hacer clic en URL peligrosas a veces se hacen pasar por correos electrónicos de bancos, proveedores de servicios de Internet o corporaciones conocidas.
2. Ataques de malware: Los ataques de malware ocurren cuando se introduce software malicioso en un sistema informático con la intención de dañarlo, infectarlo o tomar el control del mismo sin el conocimiento del usuario. Estos ataques pueden adoptar diversas formas, como spyware, ransomware, gusanos y virus. Sitios web infectados, archivos adjuntos de correo electrónico infectados, unidades USB infectadas y otros canales pueden utilizarse para transmitir el malware. Una vez que el malware se ha instalado en un sistema, puede robar datos confidenciales, corromper programas y archivos, tomar el control remoto del dispositivo o exigir un rescate para desbloquear los datos.
3. Ataques de denegación de servicio (DoS): Los ataques de denegación de servicio (DoS) son un tipo de ataque malicioso que tiene como objetivo interrumpir o evitar el acceso legítimo a recursos al inundar un sistema o una red con un exceso de tráfico o solicitudes falsas. Estos ataques buscan agotar los recursos disponibles, como el ancho de banda, la capacidad de procesamiento o la memoria, impidiendo que los usuarios legítimos accedan a los servicios o páginas web afectadas. Los ataques de denegación de servicio pueden llevarse a cabo utilizando diferentes técnicas, como inundación de paquetes, ataques de amplificación, ataques de agotamiento de recursos o ataques distribuidos de denegación de servicio (DDoS), que involucran múltiples dispositivos coordinados para lanzar el ataque. El objetivo principal de estos ataques es interrumpir la disponibilidad y el funcionamiento normal de los sistemas y servicios afectados, causando inconvenientes a los usuarios legítimos y posibles pérdidas financieras para las organizaciones afectadas. Ingeniería social: este tipo de hacking implica manipular a las personas para obtener acceso no autorizado a información confidencial o sistemas. Los piratas informáticos utilizan estrategias psicológicas para engañar a los usuarios y obtener información relevante.
4. Ataques de fuerza bruta: los ataques de fuerza bruta son intentos maliciosos de obtener acceso no autorizado a un sistema o cuenta mediante la realización sistemática de intentos de todas las combinaciones posibles de nombres de usuario, contraseñas o claves de encriptación hasta encontrar la correcta. En estos ataques se utilizan herramientas o scripts automatizados para generar y enviar rápidamente un gran número de intentos de inicio de sesión o desencriptación. El objetivo del atacante es obtener acceso no autorizado aprovechando credenciales débiles o fáciles de adivinar. Los ataques de fuerza bruta pueden dirigirse a diversos tipos de sistemas, como sitios web, cuentas en línea, dispositivos de red y archivos encriptados. Son especialmente

efectivos contra contraseñas débiles o mal protegidas. Para mitigar el riesgo de ataques de fuerza bruta, se pueden implementar medidas de seguridad como políticas de contraseñas fuertes, bloqueo de cuentas después de varios intentos fallidos de inicio de sesión y autenticación de múltiples factores.

5. Hackeo de redes inalámbricas: El acto de acceder ilegalmente a una red WiFi sin el permiso del propietario se conoce como hackeo de redes inalámbricas. Se utilizan métodos de ingeniería social o se aprovechan las fallas en el protocolo de seguridad de la red para obtener la contraseña de acceso.

Existen diversas estrategias utilizadas para hackear redes inalámbricas, como el uso de programas de rompimiento de contraseñas, el empleo de ataques de diccionario que prueban múltiples combinaciones de contraseñas, aprovechar las debilidades en el protocolo de seguridad WEP o WPA, y clonar direcciones MAC para suplantar la identidad de un dispositivo autorizado.

Si un hacker logra penetrar exitosamente en una red inalámbrica, podrá acceder a los datos, contraseñas, correos electrónicos y actividades en línea que se transmiten a través de la red. También pueden llevar a cabo actividades maliciosas, como distribuir malware, interceptar el tráfico de la red o realizar ataques de phishing.

6. Hackeo de aplicaciones: El acto de acceder ilegalmente a un software o una aplicación sin el permiso del propietario se conoce como hackeo de aplicaciones. En este tipo de ataque, se puede manipular o explotar el código de la aplicación, robar credenciales de acceso o realizar modificaciones no autorizadas en los datos o funcionalidades. Los hackers pueden utilizar diversas técnicas y herramientas para llevar a cabo el hackeo de aplicaciones, como el análisis inverso para investigar y comprender el funcionamiento interno de la aplicación, la inyección de código malicioso para obtener acceso no autorizado o el uso de técnicas de hackeo de contraseñas para obtener credenciales de usuario. Una vez que un hacker ha logrado hackear una aplicación con éxito, puede acceder a información sensible almacenada dentro de la aplicación, como datos personales, registros de actividades o información financiera. Además, pueden modificar la funcionalidad de la aplicación, introducir malware o cometer fraudes.

7. Hackeo de cuentas: El hackeo de cuentas es el acto ilegal de acceder a la cuenta de otra persona sin su permiso. Esto puede incluir el acceso no autorizado a diferentes tipos de cuentas, como correo electrónico, juegos en línea o cuentas bancarias en línea. Los hackers utilizan diversos métodos para hackear cuentas, como adivinar contraseñas, realizar ataques de fuerza bruta, llevar a cabo estafas de phishing, registrar pulsaciones de teclas y utilizar ingeniería social. Estas técnicas tienen como objetivo obtener o adivinar las credenciales de la cuenta, eludir medidas de seguridad o manipular al usuario para que revele su información de inicio de sesión. Una vez que un hacker logra acceder con éxito a una cuenta, puede utilizarla de diversas formas. Puede robar información personal, enviar correos electrónicos no deseados o de phishing, realizar transacciones no autorizadas, distribuir malware o hacerse pasar por el titular de la cuenta para cometer fraudes.

Se debe tener en cuenta que la piratería informática es ilegal y puede tener graves repercusiones financieras y legales para los hackers. Utilizar software de seguridad, mantener los sistemas actualizados y utilizar contraseñas únicas y fuertes son medidas que los particulares y las empresas pueden tomar para proteger sus datos y sistemas.

4.3. Daños causados por la piratería

La piratería informática puede causar daños tanto a nivel individual como empresarial de diversas formas. Algunos ejemplos de los posibles daños que puede causar la piratería son:

1. Disminución de ingresos: La disminución de ingresos debido a la piratería puede tener un efecto significativo tanto en las empresas como en los creadores de contenido. La piratería puede reducir los ingresos por varias razones, incluyendo:
 - 1.1.- Reducción de ventas: Cuando los consumidores tienen acceso gratuito a contenido pirateado, es menos probable que paguen por el mismo contenido. Esto puede llevar a una reducción en las ventas reales de productos o servicios.
 - 1.2.- Competencia desleal: Los vendedores legítimos, que deben cubrir los costos de producción y distribución, pueden ser perjudicados por los piratas que ofrecen contenido pirateado a precios muy bajos o de forma gratuita. Se crea una competencia desleal, lo que puede resultar en pérdidas económicas para los negocios legítimos.
 - 1.3.- Disminución de la inversión en nuevo contenido: Cuando los ingresos se ven afectados por la piratería, las empresas y los creadores de contenido pueden tener menos recursos para invertir en la creación de nuevo contenido o en mejorar la calidad del contenido existente. Esto puede afectar negativamente la cantidad y calidad del contenido disponible.
 - 1.4.- Efecto en la industria en general: El robo no solo afecta a las empresas y creadores individuales, sino que también tiene un impacto negativo en toda la industria. Si la piratería causa una disminución general en los ingresos, esto puede resultar en despidos, menos oportunidades para nuevos talentos y una menor inversión en investigación y desarrollo.
2. Amenazas a la seguridad: La piratería puede presentar una serie de riesgos de seguridad, que incluyen:
 - 2.1.- Virus y malware: El contenido pirateado a menudo se distribuye a través de sitios web, plataformas de intercambio de archivos o redes de igual a igual y puede estar infectado con malware o virus. Al descargar y ejecutar archivos piratas, los usuarios corren el riesgo de infectar sus dispositivos con software malicioso que puede comprometer su seguridad y privacidad.
 - 2.2.- Engaño y falsificación: Los piratas pueden alterar el contenido original para incluir elementos falsificados o engañosos, como anuncios maliciosos, enlaces a sitios web fraudulentos o contenido manipulado. Esto puede hacer que los usuarios sean víctimas de estafas, ataques de phishing o robo de identidad.
 - 2.3.- Divulgación de información personal: Acceder a servicios o plataformas pirateadas puede requerir que los usuarios proporcionen información personal o credenciales de inicio de sesión, como contraseñas o números de tarjeta de crédito. Esto pone en riesgo su privacidad y los expone al robo de identidad o fraude financiero.
 - 2.4.- Vulnerabilidades de software: El uso de software pirateado implica la omisión de actualizaciones de seguridad y parches. Esto deja a los usuarios expuestos a vulnerabilidades conocidas y puede facilitar el acceso no autorizado a sus dispositivos o redes.
 - 2.5.- Riesgos legales: Involucrarse en actividades de piratería, ya sea como proveedor o usuario, puede tener graves consecuencias legales. Las autoridades encargadas de

- hacer cumplir la ley pueden rastrear y emprender acciones legales contra aquellos involucrados en la distribución o consumo de contenido pirateado.
3. Daño a la reputación: El daño a la reputación debido a la piratería puede tener impactos significativos. Algunos de los efectos negativos en la reputación causados por la piratería incluyen:
 - 3.1.- Percepción de baja calidad: El contenido pirateado a menudo es de calidad inferior, ya que con frecuencia se obtiene de fuentes no autorizadas sin cumplir con los estándares de producción adecuados. Esto puede llevar a los consumidores a asociar el contenido pirateado con baja calidad, lo cual afecta la reputación de los creadores legítimos.
 - 3.2.- Pérdida de confianza pública: Cuando los consumidores descubren que una empresa o creador está involucrado en la distribución o promoción de contenido pirateado, puede resultar en una pérdida de confianza en la marca. Esto puede afectar la relación con los clientes y tener un impacto negativo en la imagen y reputación de la empresa.
 - 3.3.- Impacto en la industria: La piratería no solo afecta a una empresa individual, sino que también puede dañar la reputación de toda una industria. Si se percibe que una industria está plagada de contenido pirateado, puede provocar una pérdida de confianza pública y una disminución del valor percibido de los productos y servicios legítimos.
 - 3.4.- Responsabilidad legal y sanciones: Participar en actividades de piratería puede tener consecuencias legales y sanciones, lo cual a su vez puede afectar la reputación de una empresa o creador. Estar asociado con prácticas ilegales puede dañar la credibilidad y prestigio de una marca.
 4. Violación de la privacidad: La piratería puede dar lugar a violaciones de privacidad de varias maneras:
 - 4.1.- Divulgación no autorizada de información personal: La distribución en línea de contenido pirateado puede contener información privada y sensible de creadores u propietarios legítimos. Ejemplos de esta información incluyen direcciones de correo electrónico, contraseñas, información de tarjetas de crédito u otros datos confidenciales. Estos datos pueden ser utilizados de manera malintencionada, como para cometer fraudes o robo de identidad.
 - 4.2.- Acceso no autorizado a dispositivos: Los usuarios pueden poner en riesgo sus dispositivos al descargar o utilizar contenido pirateado, ya que esto puede llevar a la instalación de virus o software malicioso. Estos programas pueden comprometer la seguridad de los dispositivos y permitir que los hackers accedan a información personal almacenada en ellos, como archivos, fotos, contactos o historial de navegación.
 - 4.3.- Riesgo de espionaje: Al utilizar servicios o plataformas pirateadas, los usuarios corren el riesgo de que sus actividades en línea sean monitoreadas y registradas sin su conocimiento o consentimiento. Esto puede incluir el seguimiento de la navegación, acceso a mensajes o correos electrónicos, e incluso la grabación de conversaciones y llamadas privadas.
 - 4.4.- Exposición a estafas y phishing: Los sitios web o plataformas que ofrecen contenido pirateado pueden estar diseñados para engañar a los usuarios y obtener información personal sensible a través de técnicas de phishing. Los usuarios pueden ser redirigidos a ingresar información confidencial, como contraseñas o datos bancarios, en páginas falsas que pretenden ser legítimas.

5. Interrupción de servicios: Los ataques de piratería informática, como los ataques de denegación de servicio (DoS), pueden interrumpir el funcionamiento normal de servicios en línea. Los servicios pueden ser interrumpidos de varias formas debido a la piratería:
 - 5.1.- Sobrecarga de servidores: Compartir contenido pirateado en línea puede generar una gran cantidad de solicitudes de descarga y tráfico en los servidores. Esto puede provocar una sobrecarga en los servidores, lo que resulta en un rendimiento reducido o incluso en la caída de los servicios legítimos.
 - 5.2.- Inestabilidad del sistema: Existe el riesgo de que las versiones pirateadas de software o aplicaciones estén mal desarrolladas o contengan errores. Esto puede llevar a la inestabilidad del sistema, causando fallas o bloqueos que interrumpen el funcionamiento normal de los servicios.
 - 5.3.- Pérdida de ingresos para los proveedores de servicios: La piratería puede reducir los ingresos de los proveedores de servicios legítimos, lo que a su vez puede afectar su capacidad para mantener y mejorar la calidad de los servicios ofrecidos. Esto puede resultar en una disminución en la disponibilidad o calidad de los servicios para los usuarios legítimos.
 - 5.4.- Agotamiento de recursos: Compartir contenido pirateado a través de redes peer-to-peer o sitios de intercambio de archivos consume una cantidad significativa de ancho de banda y espacio de almacenamiento. Esto puede agotar los recursos disponibles para los usuarios legítimos, lo que resulta en una reducción de la velocidad de conexión o un aumento en la congestión de la red.
6. Pérdida de propiedad intelectual: La piratería informática puede dar lugar al robo de propiedad intelectual de diversas formas:
 - 6.1.- Copia sin autorización: La piratería informática implica la copia y distribución no autorizada de software, música, películas u otro tipo de contenido protegido por derechos de autor. Esto resulta en una pérdida directa de propiedad intelectual para los creadores legítimos.
 - 6.2.- Infracción de derechos de autor: Al piratear software o contenido protegido por derechos de autor, se violan los derechos exclusivos del titular de los derechos. Esto puede incluir el derecho de reproducción, distribución o ejecución pública de la obra. La piratería informática priva a los creadores del reconocimiento y los ingresos que merecen por su trabajo.
 - 6.3.- Divulgación no autorizada de secretos comerciales: En algunos casos, la piratería informática puede implicar el acceso y divulgación no autorizados de información confidencial o secretos comerciales de empresas. Esto puede resultar en una pérdida significativa de propiedad intelectual y ventaja competitiva para las organizaciones afectadas.
 - 6.4.- Declive de oportunidades comerciales: Cuando se piratea software o contenido, los creadores legítimos pierden la capacidad de controlar y monetizar su propiedad intelectual. Esto puede limitar las oportunidades comerciales, como licencias, asociaciones o acuerdos de distribución, lo que tiene un impacto negativo en los ingresos y el crecimiento.
7. Costos de cumplimiento legal: Los costos de cumplimiento legal relacionados con la piratería informática pueden tener un impacto significativo, incluyendo:
 - 7.1.- Demandas y acciones legales: Los titulares de derechos de autor y las empresas afectadas por la piratería informática a menudo emprenden acciones legales para proteger sus derechos y buscar compensación por las pérdidas sufridas. Esto puede

implicar costos legales significativos, como honorarios de abogados, gastos de litigio y posibles multas.

7.2.- Implementación de medidas de seguridad y protección: Para protegerse contra la piratería informática y evitar posibles sanciones legales, las empresas deben invertir en la implementación de medidas de seguridad y protección para sus sistemas y contenido digital. Esto puede incluir la adquisición de software de seguridad, la contratación de expertos en ciberseguridad y la implementación de políticas y procedimientos adecuados.

7.3.- Educación y capacitación en cumplimiento legal: Para garantizar el cumplimiento de las leyes de propiedad intelectual y derechos de autor, las empresas deben capacitar a su personal en las normas y regulaciones pertinentes. Esto puede requerir recursos dedicados a programas de educación y capacitación, así como actualizaciones periódicas de conocimientos y políticas de cumplimiento.

7.4.- Monitoreo y detección de infracciones: Las empresas deben asignar recursos para monitorear y detectar posibles infracciones de propiedad intelectual y piratería informática. Esto puede implicar el uso de herramientas de monitoreo, análisis de datos y seguimiento de actividades sospechosas en línea.

Un gran ejemplo de estos daños fue el caso de Sony Pictures Entertainment. En 2014, Sony Pictures Entertainment fue víctima de un ataque cibernético masivo atribuido a piratas informáticos respaldados por el gobierno de Corea del Norte. Los hackers filtraron gran cantidad de información confidencial, incluyendo correos electrónicos, contratos y películas no lanzadas, lo que provocó daños significativos a la reputación de la compañía y pérdidas financieras.

4.4. Herramientas contra la piratería

Existen diferentes herramientas para la protección contra la piratería que pueden ayudar a defender los sistemas y el contenido digital, algunos de los más relevantes son:

1. Software de seguridad: El software de seguridad se refiere a programas diseñados para proteger sistemas informáticos y datos contra amenazas y ataques cibernéticos. Estos programas se utilizan para prevenir, detectar y responder a diferentes formas de malware, como virus, troyanos, spyware y ransomware, así como para proteger contra vulnerabilidades de seguridad y ataques de hackers.

El software de seguridad puede incluir:

1.1.- Antivirus: Los programas antivirus están diseñados para detectar y eliminar virus y otros tipos de malware de los sistemas informáticos.

1.2.- Firewall: Un firewall es una barrera de seguridad que monitorea y controla el tráfico de red, bloqueando o permitiendo el acceso según reglas de seguridad establecidas.

1.3.- Antispyware: El software antispyware ayuda a detectar y eliminar spyware y programas no deseados que recopilan información sin el consentimiento del usuario.

1.4.- Antimalware: Estos programas están diseñados para proteger contra una amplia gama de malware, incluyendo virus, gusanos, troyanos y ransomware.

1.5.- Protección de navegación: Algunos softwares de seguridad ofrece funciones de protección de navegación que bloquean sitios web maliciosos y advierten sobre posibles amenazas de seguridad al navegar por Internet.

2. Administración de derechos digitales (DRM): El ³⁰La Administración de Derechos Digitales (DRM) se refiere a un conjunto de tecnologías y procedimientos utilizados para regular el acceso, uso y distribución de contenido digital protegido por derechos de autor. El DRM se implementa con el objetivo de proteger los derechos de los creadores y propietarios de contenido, al tiempo que limita la copia no autorizada y la redistribución ilegal.

Las características y funciones comunes del DRM se componen de:

2.1.- Seguridad de copia: El DRM puede incorporar mecanismos que limitan o impiden la copia no autorizada de contenido digital, como películas, música, libros electrónicos, software, entre otros.

2.2.- Gestión de licencias: El sistema de administración de derechos digitales permite a los proveedores de contenido obtener licencias específicas para el acceso y uso del contenido. Estas licencias pueden incluir restricciones sobre la cantidad de dispositivos en los que se puede reproducir el contenido, el período de tiempo durante el cual se puede acceder al contenido y otras condiciones de uso.

2.3.- Encriptación: El DRM utiliza la encriptación como medio para proteger los archivos digitales, dificultando el acceso no autorizado o la modificación.

2.4.- Autenticación y verificación de usuarios: El DRM puede requerir la autenticación de usuarios antes de permitirles acceder al contenido protegido. Esto ayuda a prevenir la distribución ilegal y el acceso no autorizado.

2.5.- Restricciones de distribución y reproducción: El DRM puede imponer restricciones en la distribución y reproducción del contenido digital. Esto puede incluir limitaciones en la cantidad de veces que se puede reproducir el contenido o la capacidad de compartirlo con otros usuarios.

3. Firmas electrónicas: Una técnica para verificar la identidad de una persona o entidad en entornos digitales es la firma electrónica. Se utiliza para firmar documentos electrónicos y proporciona confianza y seguridad en transacciones en línea.

Las firmas electrónicas tienen las siguientes características:

3.1.- Autenticidad: Con una firma electrónica se puede verificar la identidad del firmante, asegurando que el documento ha sido firmado por la persona o entidad correcta.

3.2.- Integridad: La firma electrónica garantiza que no se han realizado cambios en el documento desde que fue firmado. Cualquier modificación realizada después de la firma será detectable.

3.3.- No repudio: Una vez que se ha aplicado una firma electrónica a un documento, el firmante no puede negar su autoría. Esto proporciona un registro de la transacción y evita disputas legales.

3.4.- Seguridad: Las firmas electrónicas utilizan técnicas criptográficas para proteger la información y prevenir falsificaciones. Se emplean algoritmos y claves criptográficas para garantizar la seguridad de la firma.

Las firmas electrónicas son reconocidas legalmente en muchos países y se utilizan en una amplia gama de transacciones, como contratos, acuerdos comerciales, solicitudes en línea, declaraciones de impuestos, entre otros.

4. Actualización de software: Las actualizaciones de software también son fundamentales porque pueden ayudar a combatir y prevenir el uso no autorizado de software y

³⁰ Digital Rights Management (DRM)

contenido protegidos por derechos de autor. Aquí hay algunas consideraciones importantes:

- 4.1.- Actualizaciones de seguridad: Los desarrolladores de software lanzan regularmente actualizaciones de seguridad para solucionar vulnerabilidades conocidas. Estas actualizaciones pueden corregir fallas que podrían ser explotadas por piratas informáticos para acceder ilegalmente a software protegido o evadir medidas de seguridad.
- 4.2.- Mejoras en la protección contra copias: Los creadores de software a menudo incluyen mejoras en las actualizaciones para fortalecer la protección contra copias de sus productos. Estas mejoras pueden dificultar la piratería y la distribución no autorizada de software.
- 4.3.- Actualizaciones de licencias: Algunos programas utilizan sistemas de gestión de licencias que requieren actualizaciones periódicas para verificar la autenticidad y validez de las licencias. Estas actualizaciones pueden ayudar a prevenir el uso de licencias piratas o no autorizadas.
- 4.4.- Detección y bloqueo de versiones pirateadas: Algunas actualizaciones de software incluyen medidas para detectar y bloquear versiones piratas o no autorizadas del programa. Estas medidas pueden ayudar a proteger los intereses de los desarrolladores y fomentar el uso legal del software.
5. Protección de derechos de autor: La protección de los derechos de autor es una parte fundamental en la lucha contra la piratería y la salvaguardia de la propiedad intelectual. A continuación, se presentan algunas consideraciones importantes relacionadas con la protección de los derechos de autor:
 - 5.1.- ³¹Registro de derechos de autor: Registrar obras creativas y originales ante las autoridades de propiedad intelectual brinda evidencia legal de la titularidad y es una herramienta importante en caso de disputas o infracciones.
 - 5.2.- Aviso de derechos de autor: Incluir avisos de derechos de autor en el contenido protegido puede disuadir a los infractores y recordarles que el material está legalmente protegido.
 - 5.3.- Acciones legales: Los titulares de derechos de autor pueden emprender acciones legales contra aquellos que infringen sus derechos. Esto puede incluir presentar demandas, obtener órdenes de cese y desistimiento y buscar compensación por daños.
 - 5.4.- Educación y concienciación: Es importante educar a la sociedad sobre la importancia de respetar los derechos de autor y los efectos negativos de la piratería. Esto puede incluir campañas de concienciación, programas educativos y promover una cultura de respeto por la propiedad intelectual.
 - 5.5.- Colaboración con plataformas en línea: Las plataformas en línea desempeñan un papel crucial en la protección de los derechos de autor. Colaborar con estas plataformas para implementar medidas de protección, como detectar y eliminar contenido pirateado, puede ser eficaz en la lucha contra la piratería.
6. Verificación de usuarios: La verificación de usuarios puede desempeñar un papel importante en la prevención y detección de actividades ilícitas. Algunas características particulares de la verificación de usuarios son:
 - 6.1.- Acceso restringido: La implementación de un proceso de verificación de usuarios puede ayudar a restringir el acceso a contenido protegido por derechos de autor. Al requerir que los usuarios se autentifiquen antes de acceder al contenido, se

³¹ Ministerio de Cultura y Deporte. (s.f.). ¿Qué es la propiedad intelectual?.

puede reducir la probabilidad de que personas no autorizadas obtengan y compartan material pirateado.

6.2.- Identificación de infractores: A través de la verificación de usuarios, se puede obtener información sobre la identidad de las personas que acceden a una plataforma o servicio. Esto puede ser útil para identificar a los infractores de derechos de autor y tomar medidas legales en su contra.

6.3.- Seguimiento de actividades: La verificación de usuarios permite realizar un seguimiento de las actividades en línea, lo que ayuda a detectar patrones sospechosos relacionados con la piratería. Esto incluye monitorear descargas ilegales, identificar cuentas que comparten contenido no autorizado y registrar información que pueda utilizarse como evidencia en investigaciones legales.

6.4.- Prevención de uso no autorizado: Mediante la implementación de métodos de verificación de usuarios, se puede dificultar el uso no autorizado de software, aplicaciones o servicios. Esto ayuda a prevenir la instalación y uso de versiones pirateadas de software, protegiendo así los derechos de autor y la propiedad intelectual.

7. Vigilancia de actividad sospechosa: La vigilancia de actividades sospechosas es una medida importante en la lucha contra la piratería y la protección de los derechos de autor. A continuación se presentan algunas consideraciones relacionadas con esta vigilancia:

7.1.- Monitoreo de la red: Observar las redes informáticas y los sistemas puede ayudar a identificar patrones y actividades sospechosas que puedan estar relacionadas con la piratería. Esto implica analizar el uso de aplicaciones, monitorear el tráfico de la red e identificar actividades inusuales o no autorizadas.

7.2.- Identificación de infracciones: Mediante el uso de herramientas y tecnologías de detección, es posible identificar infracciones de derechos de autor, como la descarga o distribución no autorizada de contenido protegido. Esto permite tomar medidas rápidas para detener la propagación de contenido pirateado y proteger los intereses de los creadores.

7.3.- Colaboración con proveedores de servicios en línea: Trabajar en conjunto con proveedores de servicios en línea, como plataformas de contenido o redes sociales, puede ser beneficioso para identificar y abordar actividades sospechosas relacionadas con la piratería. Establecer mecanismos de informe y responder de manera efectiva a los informes de infracción puede ayudar a proteger los derechos de autor.

7.4.- Uso de herramientas de filtrado y análisis: La implementación de herramientas de análisis y filtrado permite identificar contenido pirateado o no autorizado en plataformas en línea. Esto facilita la eliminación y bloqueo de dicho contenido, protegiendo los derechos de autor y evitando su distribución ilícita.

En cuanto a las acciones legales que se pueden emprender contra los hackers o las herramientas jurídicas que protegen a la sociedad de los delincuentes informáticos se encuentran:

1. Leyes de derechos de autor: Las leyes de derechos de autor otorgan protección legal a los creadores y titulares de derechos sobre sus obras originales. Estas leyes establecen los derechos exclusivos de reproducción, distribución, exhibición y realización pública, entre otros, y permiten emprender acciones legales contra aquellos que infrinjan dichos derechos.
2. Legislación antipiratería: Muchos países cuentan con leyes específicas que prohíben y penalizan la piratería informática y la infracción de derechos de autor. Estas leyes pueden

incluir sanciones civiles y penales, así como medidas para la confiscación de equipos utilizados para cometer infracciones.

3. Tratados internacionales: Existen tratados internacionales, como el ³²Convenio de Berna y el Tratado de la OMPI³³ sobre Derecho de Autor, que armonizan las normas de protección de los derechos de autor a nivel global. Estos tratados permiten a los países miembros tomar medidas legales contra la piratería y proporcionan un marco de cooperación internacional para combatir la infracción.
4. Acciones civiles: Los titulares de derechos pueden emprender acciones civiles contra los infractores, buscando indemnizaciones por daños y perjuicios, así como la cesación de la actividad infractora. Estas acciones suelen llevarse a cabo a través de demandas judiciales y pueden requerir la asistencia de abogados especializados en propiedad intelectual.
5. Cooperación con autoridades: Los titulares de derechos pueden colaborar con las autoridades competentes, como la policía y las agencias de aplicación de la ley, para denunciar y perseguir los casos de piratería. Esto implica proporcionar pruebas, testimonios y cualquier otra información relevante que ayude a las investigaciones y procesos legales.
6. Medidas tecnológicas de protección: Algunos países cuentan con legislación que prohíbe la elusión de medidas tecnológicas de protección (TPM, por sus siglas en inglés) utilizadas para proteger los derechos de autor, como el cifrado o los sistemas de gestión de derechos digitales (DRM). Estas medidas buscan evitar la vulneración de la protección tecnológica implementada en el contenido digital.

No obstante, pese a todas estas medidas contra la piratería, cabe recalcar que la mejor forma de prevenir efectivamente la piratería y reducir los riesgos, es implementar una combinación de medidas técnicas, legales y de concienciación pública, ya que, si el usuario no está concienciado de las acciones que lo exponen ante los ciberdelincuentes, toda protección va a ser mucho más complicada.

5. Fiscalización y sanciones

5.1. Fiscalización del software en España

En España, la supervisión del software está llevada a cabo por diferentes entidades y está regulada por varias normativas y directrices. En España, algunos de los aspectos importantes de la supervisión del software consisten en:

1. Protección de la Información: La Agencia Española de Protección de Datos (AEPD) se encarga de garantizar que las empresas y organizaciones manejen los datos personales de acuerdo con las regulaciones vigentes y supervisa el cumplimiento de la Ley Orgánica de Protección de Datos. Algunas consideraciones importantes para proteger la información durante la supervisión del software:

³² Convenio de Berna para la Protección de las Obras Literarias y Artísticas (1886). Organización Mundial de la Propiedad Intelectual.

³³ Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor (1996). Organización Mundial de la Propiedad Intelectual.

- 1.1.- Privacidad y confidencialidad: Es fundamental respetar la privacidad de los usuarios y garantizar la confidencialidad de los datos recopilados durante la supervisión. Esto requiere el uso de técnicas y herramientas que salvaguarden los datos personales y respeten la privacidad.
- 1.2.- ³⁴Pseudonimización de datos: Se deben utilizar técnicas de pseudonimización al recopilar datos con fines de supervisión para eliminar cualquier información de identificación personal. Esto ayuda a proteger la privacidad de los usuarios durante la supervisión necesaria.
- 1.3.- Cumplimiento de regulaciones de protección de datos: Al realizar la supervisión del software, es importante cumplir con las leyes y regulaciones de protección de datos, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Esto implica obtener el consentimiento adecuado del usuario y garantizar la privacidad y seguridad de los datos recopilados.
- 1.4.- Protección de la información: Es fundamental implementar medidas de seguridad adecuadas para proteger la información recopilada durante la supervisión del software. Esto puede incluir el uso de cifrado, firewalls y otras medidas de seguridad para evitar el acceso no autorizado a la información.
- 1.5.- Retención y eliminación de datos: Es importante establecer políticas claras de retención y eliminación de datos para la información recopilada durante la supervisión del software. Los datos deben mantenerse solo durante el tiempo necesario y eliminarse de manera segura una vez que ya no sean necesarios.
2. Derecho de Propiedad: El derecho de autor y los derechos relacionados con el software están protegidos por la Ley de Propiedad Intelectual. Las infracciones de los derechos de propiedad intelectual son vigiladas, controladas y sancionadas por la Comisión de Propiedad Intelectual, que forma parte del Ministerio de Cultura y Deporte. Vemos algunas consideraciones importantes relacionadas con el derecho de propiedad en la supervisión del software:
 - 2.1.- Derechos de autor: Los propietarios de software tienen el derecho exclusivo de controlar la reproducción, distribución y ejecución pública de su software mediante la protección de derechos de autor. Esto incluye el derecho a supervisar cómo se utiliza el software y tomar medidas para protegerlo contra el uso no autorizado.
 - 2.2.- Licencias de software: Al distribuir software, los propietarios pueden establecer condiciones y restricciones específicas a través de acuerdos de licencia de software. Estas licencias pueden incluir disposiciones que permitan la supervisión y vigilancia del software para garantizar el cumplimiento de los términos de uso y detectar posibles infracciones.
 - 2.3.- Tecnologías de protección de software: Los propietarios de software pueden utilizar tecnologías de protección de software, como medidas de gestión de derechos digitales (DRM), para supervisar y controlar el uso del software. Estas tecnologías pueden incluir características como verificación de licencias, restricciones de copia y seguimiento de actividades para garantizar el cumplimiento de los términos de uso.
 - 2.4.- Privacidad y derechos de los usuarios: Además de los derechos de propiedad del software, también es importante respetar la privacidad y los derechos de los usuarios. La supervisión del software debe llevarse a cabo de manera ética y en cumplimiento de las leyes aplicables de protección de datos y privacidad. Los propietarios deben

³⁴ World Compliance Association. (2017). El Reglamento Europeo de Protección de Datos: ¿Qué es la seudonimización?

- garantizar el consentimiento adecuado cuando sea necesario y proteger adecuadamente la información personal de los usuarios.
3. Seguridad para el Consumidor: La Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) se encarga de proteger los derechos de los consumidores y garantizar que el software que se comercializa cumpla con los estándares de calidad y seguridad establecidos. La seguridad para el consumidor en el software es de vital importancia para garantizar una experiencia segura y proteger la información personal de los usuarios. A continuación, se presentan algunas consideraciones importantes relacionadas con la seguridad del consumidor en el software:
 - 3.1.- Protección de datos personales: Los desarrolladores de software deben implementar medidas de seguridad para proteger los datos personales de los usuarios. Esto implica el uso de métodos de encriptación, almacenamiento seguro de datos y la implementación de políticas de privacidad claras y transparentes.
 - 3.2.- Actualizaciones de seguridad: Los desarrolladores deben proporcionar actualizaciones regulares de seguridad para abordar las vulnerabilidades conocidas y proteger a los usuarios contra amenazas cibernéticas. Estas actualizaciones pueden incluir parches de seguridad, correcciones de errores y mejoras en la protección contra malware y virus.
 - 3.3.- Autenticación y acceso seguro: Es importante que el software brinde opciones de autenticación seguras, como contraseñas robustas, autenticación de dos factores o biometría, para proteger el acceso no autorizado a las cuentas de los usuarios.
 - 3.4.- Protección contra software malicioso: Los desarrolladores deben implementar medidas para prevenir y detectar la presencia de software malicioso, como virus, malware y spyware. Esto puede incluir el uso de software de seguridad, análisis de amenazas y filtros para evitar la descarga o ejecución de software no deseado.
 - 3.5.- Transparencia en la recopilación de datos: Los desarrolladores deben ser transparentes sobre qué información se recopila y cómo se utiliza en el software. Los usuarios deben tener la opción de controlar la recopilación y el uso de sus datos personales, y deben recibir información clara sobre las políticas de privacidad y el manejo de datos.
 - 3.6.- Educación y conciencia: Los desarrolladores deben proporcionar información y recursos educativos a los usuarios para ayudarles a comprender los riesgos de seguridad y adoptar prácticas seguras en el uso del software. Esto puede incluir tutoriales, guías de seguridad y consejos para protegerse de amenazas cibernéticas.
 4. Seguridad de la Información: El Instituto Nacional de Ciberseguridad (INCIBE) tiene la tarea de promover la seguridad de la información y garantizar la protección de los sistemas informáticos en España. Esto incluye el software relacionado con la ciberseguridad y la respuesta a incidentes. Algunas de las consideraciones más importante para la seguridad de la información en el software son:
 - 4.1.- Encriptación de datos: Se debe utilizar la encriptación para proteger los datos sensibles almacenados en el software contra accesos no autorizados. La información se encripta para que solo las personas autorizadas puedan acceder y leerla.
 - 4.2.- Acceso y autenticación seguros: Los sistemas de software deben implementar métodos de autenticación seguros, como biometría, autenticación de dos factores o contraseñas robustas, para garantizar que solo los usuarios autorizados tengan acceso a los datos.
 - 4.3.- Gestión de acceso y privilegios: Es importante implementar controles de acceso y privilegios para garantizar que los usuarios solo tengan acceso a la información y

funciones necesarias para realizar sus tareas. Esto reduce el riesgo de filtración de información y previene accesos no autorizados.

4.4.- Seguridad contra amenazas externas: El software debe contar con medidas de seguridad para protegerse contra amenazas externas como ataques de hacking, malware y phishing. Esto puede incluir firewalls, sistemas de detección de intrusiones y software antivirus actualizado.

4.5.- Parches y actualizaciones de seguridad: Los desarrolladores de software deben proporcionar parches y actualizaciones de seguridad de manera regular para solucionar vulnerabilidades conocidas y protegerse contra nuevas amenazas. Los usuarios deben mantener su software actualizado para beneficiarse de las últimas mejoras de seguridad.

4.6.- Auditoría y monitoreo de eventos: Al incorporar sistemas de auditoría y monitoreo en el software, se pueden identificar actividades sospechosas o inusuales y tomar medidas para abordarlas. Esto ayuda a identificar intentos de acceso no autorizado o comportamientos anómalos que puedan indicar una brecha de seguridad.

4.7.- Respaldo y recuperación de datos: Es fundamental contar con procedimientos adecuados de respaldo y recuperación de datos para garantizar la disponibilidad e integridad de la información en caso de pérdida, daño o corrupción de datos.

Desde el diseño hasta la implementación y el mantenimiento continuo, la seguridad de la información en el software debe ser una prioridad. Los desarrolladores de software, los administradores del sistema y los usuarios deben trabajar juntos para crear y mantener un entorno seguro y protegido para la información sensible.

5.2. Sanciones por la violación de derechos de propiedad intelectual en el software

Dependiendo de las leyes del país en cuestión, las sanciones por infringir los derechos de propiedad intelectual en el software pueden variar. En casos en los que se violan los derechos de propiedad intelectual en el software, se pueden utilizar las siguientes sanciones:

1. Multas: son una de las formas más comunes de castigo por infringir los derechos de propiedad intelectual del software es una multa. Las multas pueden variar desde sanciones civiles, donde se exige al infractor que pague una compensación económica al titular de los derechos de autor afectados, hasta sanciones penales, donde se imponen multas más severas y, en algunos casos, pueden incluir penas de prisión. La gravedad de la infracción, el alcance de la violación y las leyes específicas del país influyen en la determinación del monto de la multa.
2. Daños y perjuicios: Además de las multas, es posible que se requiera que la parte infractora compense al titular de los derechos. Los daños y perjuicios pueden incluir:
 - 2.1.- Daños económicos: Esto puede incluir la pérdida de ventas, la disminución del valor del software infringido y la pérdida de ingresos por parte del titular de los derechos de autor.
 - 2.2.- Daños morales: Además de los daños económicos, el titular de los derechos de autor puede reclamar daños morales, que se refieren al daño a su reputación o imagen como resultado de la infracción.

- 2.3.- Beneficios obtenidos por el infractor: En algunos casos, el titular de los derechos de autor puede buscar obtener los beneficios económicos que el infractor haya obtenido como resultado de la infracción.
3. Confiscación de productos: En algunos casos, las autoridades pueden ordenar la confiscación de productos que violen los derechos de propiedad intelectual o contengan software ilegal. La confiscación de productos puede implicar la retirada del mercado de los productos infractores y su destrucción o disposición de otra manera autorizada por la ley. Esta medida busca evitar que los productos infractores sigan siendo comercializados y proteger los intereses del titular de los derechos de propiedad intelectual.
4. Medidas preliminares o cautelares: Los titulares de los derechos pueden solicitar al tribunal que emita una orden judicial con el objetivo evitar que la infracción continúe causando daños irreparables o dificultando la posterior ejecución de una sentencia favorable al titular de los derechos. Algunas de las medidas preliminares o cautelares comunes en casos de violación de derechos de propiedad intelectual en el software son:
- 4.1.- Orden de cese y desistimiento: Se puede solicitar una orden judicial que ordene al infractor detener inmediatamente la violación y abstenerse de llevar a cabo cualquier actividad que infrinja los derechos de propiedad intelectual.
- 4.2.- Embargo preventivo: Se puede solicitar un embargo preventivo sobre los productos o activos relacionados con la infracción, como copias ilegales del software o equipos utilizados para su producción o distribución. Esto evita que los productos infractores sean comercializados o que los activos relacionados sean utilizados para seguir infringiendo los derechos de propiedad intelectual.
- 4.3.- Incautación de pruebas: Se puede solicitar una orden judicial para incautar y preservar evidencia relevante que demuestre la violación de los derechos de propiedad intelectual. Esto puede incluir copias ilegales del software, registros de transacciones, comunicaciones o cualquier otra prueba que respalde la violación.
- 4.4.- Prohibición de importación o exportación: Se puede solicitar una prohibición sobre la importación o exportación de productos que infrinjan los derechos de propiedad intelectual. Esto impide que los productos infractores entren o salgan del territorio donde se haya solicitado la medida.
5. Responsabilidad penal: La ley puede incluir la responsabilidad penal en casos graves de violación de los derechos de propiedad intelectual en el software, especialmente aquellos relacionados con la piratería informática. Esto podría resultar en pena de prisión u otras sanciones legales por un delito incluyendo por ejemplo:
- 5.1.- Sanciones penales: La violación de derechos de propiedad intelectual en el software puede considerarse un delito penal en algunas jurisdicciones. Esto puede dar lugar a sanciones penales, que pueden incluir multas y penas de prisión para los infractores.
- 5.2.- Acciones penales por parte del titular de los derechos: El titular de los derechos de propiedad intelectual puede presentar una denuncia o demanda penal contra el infractor. Esto puede dar lugar a un proceso penal en el que el infractor puede ser declarado culpable y recibir una sentencia penal.
- 5.3.- Incautación de bienes: En algunos casos, como parte de una sentencia penal, se puede ordenar la incautación de los productos o activos relacionados con la violación de derechos de propiedad intelectual. Esto puede incluir la confiscación de copias ilegales del software, equipos utilizados para la producción o distribución del software infractor, o cualquier otro bien relacionado con la infracción.

En España estas sanciones se han llevado a cabo en multitud de casos, algunos ejemplos de ello son:

1. Copias ilegales de videojuegos: En 2018, una persona fue condenada a una pena de prisión y al pago de una multa de 5072 euros por distribuir copias ilegales de juegos de la consola PlayStation 3 y cartuchos ilegales de Nintendo en internet.
2. Uso de software pirata: En 2017, dos organizaciones que reproducían software pirata, incumpliendo con los derechos de propiedad intelectual de su/s autor/es, recibieron la mayor multa en España hasta la fecha. Esta multa supuso el pago de una indemnización de 453.800 euros en concepto de daños y perjuicios, importe correspondiente al valor de mercado de los programas sin licencia detectados, a lo que las empresas habrán de sumar los intereses legales en los que han incurrido desde la interposición de la demanda, y el pago de las costas judiciales, en total, más de 500.000 euros.

Estos son solo ejemplos de la multitud de condenas que han ido surgiendo a raíz de la piratería en España.

6. Casos prácticos

6.1. Ejemplos de casos de violación de derechos de propiedad intelectual en el software

Algunos ejemplos de casos de violación de derechos de propiedad intelectual en el software son:

1. Caso entre Microsoft y la piratería de software: Microsoft ha realizado diversas acciones legales contra personas y organizaciones involucradas en la piratería de su software. Estos casos incluyen la venta y distribución de copias ilegales de software y sistemas operativos de Microsoft.
2. Caso de Adobe y la distribución ilegal de software: Adobe Systems ha emprendido acciones legales contra personas y empresas que distribuyen versiones piratas de su software, como Photoshop, Illustrator y Acrobat. Estos casos suelen implicar la venta y distribución de copias ilegales de software de Adobe.
3. Caso de Oracle y la infracción de derechos de autor: Oracle, una empresa de software, ha presentado demandas contra varias empresas por infracción de derechos de autor relacionada con el uso no autorizado de su software y la violación de los términos de licencia.
4. Caso de Autodesk y el uso no autorizado de software: Autodesk, una empresa conocida por su software de diseño y modelado 3D, ha tomado acciones legales contra personas y empresas por el uso no autorizado de sus productos, como AutoCAD y 3ds Max.

6.2. Sentencias relevantes en materia de protección del software

A continuación, vamos a ver varias de las sentencias más relevantes y sonadas en materia de protección de software:

1. Sentencia Oracle vs. Google (2021): La Corte Suprema de los Estados Unidos confirmó que Google infringió los derechos de autor de Oracle al utilizar código de Java en su plataforma Android sin permiso.

2. Sentencia Microsoft vs. Motorola (2013): Un tribunal en Alemania dictaminó que Motorola infringió una patente de Microsoft relacionada con la tecnología de sincronización de calendario en dispositivos móviles.
3. Sentencia SAP vs. Diageo (2017): Un tribunal en el Reino Unido encontró a Diageo, una empresa de bebidas, responsable de la infracción de licencia de software al utilizar software SAP sin licencia adecuada y ordenó el pago de daños y perjuicios.
4. Sentencia Autodesk vs. Zamosc (2014): Un tribunal en Polonia determinó que Zamosc, una empresa de ingeniería infringió los derechos de Autodesk al utilizar software sin licencia y ordenó el pago de una indemnización.
5. Sentencia Adobe vs. Softman (2012): Un tribunal en México falló a favor de Adobe en un caso de infracción de derechos de autor donde Softman, una empresa de software, fue encontrada culpable de distribuir copias ilegales de software de Adobe.
6. Sentencia Nintendo vs. LoveROMs (2018): Un tribunal en los Estados Unidos emitió un fallo a favor de Nintendo en un caso de infracción de derechos de autor contra LoveROMs, un sitio web que ofrecía descargas ilegales de juegos de Nintendo.
7. Sentencia Microsoft vs. Corel Corporation (1997): En este caso, el Tribunal de Apelaciones de los Estados Unidos dictaminó que Corel había infringido los derechos de autor de Microsoft al copiar y distribuir interfaces de usuario similares a las de Microsoft Office.
8. Sentencia Apple vs. Samsung (2012): En esta disputa legal, varios tribunales de diferentes jurisdicciones, incluyendo Estados Unidos y Corea del Sur, dictaminaron que Samsung había infringido los derechos de diseño y patentes de Apple relacionados con dispositivos móviles, como el iPhone y el iPad.
9. Sentencia SAS Institute Inc. vs. World Programming Ltd. (2013): En este caso, el Tribunal de Justicia de la Unión Europea dictaminó que la reimplantación de una funcionalidad de software mediante ingeniería inversa no infringe los derechos de autor, siempre que se realice sin acceso al código fuente original.
10. Sentencia Microsoft vs. Commission (Unión Europea, 2007): En esta sentencia, la Comisión Europea multó a Microsoft por abuso de posición dominante al no proporcionar suficiente información técnica para permitir la interoperabilidad entre su sistema operativo Windows y otros productos de software.
11. Sentencia Adobe vs. Forever 21 (Estados Unidos, 2017): En esta sentencia, Adobe demandó a la cadena minorista Forever 21 por el uso no autorizado de software de Adobe. El tribunal falló a favor de Adobe y ordenó a Forever 21 a pagar una indemnización por daños y cesar el uso no autorizado del software.

7. Conclusiones

7.1. Recapitulación de los aspectos más relevantes tratados en el trabajo

La protección jurídica del software es un tema de gran relevancia en el campo de la propiedad intelectual y la tecnología. A lo largo de este Trabajo de Fin de Grado, hemos explorado diversos aspectos relacionados con esta protección, y es importante recapitular los puntos más relevantes que hemos abordado:

1. Valor del software y la necesidad de protección: El software tiene un valor económico significativo y fomenta la innovación tecnológica. Por lo tanto, es esencial proteger los derechos

de propiedad intelectual en el software para incentivar la creatividad y garantizar un entorno justo para los desarrolladores.

2. Derechos de autor y licencias de software: Hemos analizado cómo los derechos de autor desempeñan un papel crucial en la protección del software, otorgando a los creadores el control exclusivo sobre la reproducción, distribución y ejecución de su obra. Las licencias de software permiten establecer los términos y condiciones para el uso del software, brindando protección adicional y estableciendo los derechos y responsabilidades de los usuarios.

3. Medidas técnicas de protección: Hemos explorado también diferentes técnicas utilizadas para proteger el software, como la encriptación, los sistemas de gestión de derechos digitales (DRM) y las medidas de protección contra copias. Estas medidas ayudan a prevenir la piratería y el uso no autorizado del software.

4. Violación de derechos de propiedad intelectual: Hemos examinado varios tipos de violaciones de derechos de propiedad intelectual en el software, como la copia no autorizada, la distribución ilegal y la ingeniería inversa. Estas acciones pueden tener consecuencias legales significativas y perjudicar tanto a los propietarios de software como al mercado en general.

5. Consecuencias legales: En relación con las violaciones de derechos de propiedad intelectual en el software, se han presentado las posibles consecuencias legales, que pueden implicar sanciones económicas, indemnizaciones por daños y perjuicios, confiscación de productos infractores e incluso acciones penales en casos graves de infracción.

6. Marco legal: Hemos analizado el marco legal y las regulaciones a nivel nacional e internacional que respaldan la protección legal del software.

En conclusión, la protección jurídica del software es fundamental para garantizar la innovación, el respeto al derecho de autor y un mercado justo. Como resultado, hemos profundizado en los aspectos fundamentales de esta protección, examinando el derecho de autor, las licencias, las medidas técnicas, las violaciones y las consecuencias legales. Además, hemos considerado el marco legal existente a nivel tanto nacional como internacional.

7.2. Reflexiones y propuestas de mejora

Este Trabajo de Fin de Grado sobre la protección jurídica del software ha hecho que tenga consciencia de importantes hallazgos en lo que a lo legal se refiere y debido a ello también puedo realizar sugerencias para futuras investigaciones en este campo. Algunas reflexiones y propuestas de mejora son las siguientes:

Reflexiones:

1. Relevancia y complejidad: A lo largo del desarrollo de mi trabajo de fin de grado, he descubierto la complejidad y la importancia de la protección jurídica del software en el entorno actual. El software desempeña un papel crucial en la sociedad y la economía, y su protección legal es fundamental para fomentar la innovación y garantizar un entorno justo para los desarrolladores.

2. Marco normativo: Se ha observado la existencia de un marco normativo sólido en términos de propiedad intelectual y derechos de autor para proteger el software. Sin embargo, existe la necesidad de una mayor armonización entre países y actualización de las leyes para adaptarse a los avances tecnológicos y los nuevos desafíos.

3. Dificultades técnicas: El rápido avance tecnológico supone nuevos desafíos en cuanto a la protección jurídica del software. Hay áreas como la protección contra la piratería en línea y los ciberataques, que requieren especial atención y una revisión constante de las leyes y regulaciones.

Sugerencias de mejora:

1. Análisis ético: Una posible mejora sería ampliar el análisis de las implicaciones éticas en la protección jurídica del software. Esto implica considerar el equilibrio entre los derechos de propiedad intelectual y los derechos de los usuarios, así como aspectos relacionados con la privacidad, la seguridad y el acceso equitativo al software.

2. Cooperación internacional: Sugiero también el deber de investigar las posibilidades de aumentar la cooperación internacional en términos de protección jurídica del software. Esto incluye la armonización global de leyes y regulaciones, así como el intercambio de buenas prácticas y experiencias entre países.

3. Concienciación y educación: Sería muy importante bajo mi punto de vista desarrollar programas de educación y concienciación sobre la importancia de la protección jurídica del software para evitar muchos problemas que pueden surgir por el desconocimiento de los peligros existentes en materia de software. Esto incluye capacitar a usuarios y empresas sobre los riesgos de la piratería y las consecuencias legales de la infracción de derechos de autor, así como promover prácticas legales y éticas en el uso de software.

4. Estudios económicos: Realizar investigaciones sobre el impacto económico de la protección jurídica del software es importante. Esto implica analizar el efecto de la piratería en la industria del software, estrategias para la monetización de los derechos de software y medidas para fomentar la inversión y la innovación en este sector.

En conclusión, este Trabajo de Fin de Grado me ha ayudado a comprender la importancia de la protección jurídica del software y a poder identificar áreas de mejora en futuras investigaciones. Al reflexionar sobre los hallazgos y proponer mejoras, quizá haya podido contribuir también a fortalecer la protección jurídica del software y promover un entorno digital seguro y equitativo para todos los actores involucrados.

7.3. Posibles líneas de investigación futura

En relación con el tema trabajado en este trabajo de fin de grado de la protección jurídica del software, sería bueno abordarlo desde otras direcciones en el futuro para poder tener comprensión más amplia sobre el tema y abordar problemas pertinentes. Algunas líneas de investigación futura podrían ser:

1. Análisis de la eficacia de las leyes y regulaciones actuales: Examinar la eficacia de las leyes y regulaciones actuales para la protección jurídica del software. Determinar si logran su objetivo de proteger los derechos de propiedad intelectual y cómo se aplican, así como identificar posibles áreas de mejora.

2. Marco legal para el software que utiliza inteligencia artificial y aprendizaje automático: Investigar cómo se protegen legalmente los sistemas de inteligencia artificial y aprendizaje automático. Evaluar si las leyes actualmente vigentes son suficientes para abordar las

dificultades particulares que plantean estas tecnologías y sugerir posibles modificaciones legales.

3. Privacidad y seguridad de datos en el software: Examinar la relación entre la privacidad del usuario y la seguridad de los datos y la protección jurídica del software. Analizar las pautas existentes, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, y examinar cómo se aplican a los programas informáticos. Además, investigar medidas adicionales de seguridad de datos en el software.

4. Marco legal para la legalidad del software de código abierto: Examinar las protecciones para los derechos de propiedad intelectual proporcionadas por el marco legal del software de código abierto. Analizar los obstáculos legales y las mejores prácticas para el desarrollo y la distribución de software de código abierto, así como las licencias de software de código abierto más utilizadas, como la Licencia Pública General de GNU (GPL).

5. Aspectos éticos de la protección jurídica del software: Examinar las repercusiones éticas de la protección jurídica del software, como la preservación de la privacidad y la transparencia en la toma de decisiones en el uso de software, así como el equilibrio entre los derechos de propiedad intelectual y el acceso a la información. Investigar las posibilidades de incorporar consideraciones éticas en el marco legal existente.

Estas son solo algunas ideas para posibles líneas de investigación futura en el campo de la protección jurídica del software ya que se pueden ocurrir diferentes perspectivas desde las que abordar el tema.

8. BIBLIOGRAFIA.

- Aldana, A. C. A., & Cuervo, M. C. (2009). Propiedad intelectual y derechos de autor en el software libre. *Revista Virtual Universidad Católica del Norte*, (28).
- Álvarez-Cabrera, S. F., & Reyes-Hernández, K. Y. (2017). Protección jurídica de los videojuegos a través del derecho de autor. *Opinión Jurídica*, 16(31), 155-174.
- Arimetrics. (s.f.). Software. En *Glosario Digital*.
- Ayuda Ley Protección Datos. (s.f.). Patentes de software.
- Barceló García, M. (2001). Piratería informática. *Byte España*, (73), 128-128.
- Barrero J., R. (2007). La protección jurídica del software.
- Belén Gimeno, S. (14 de septiembre de 2022). Software libre vs. software open source. *Aranova*.
- Brocca, J. C., & Casamiquela, R. (2005). Las licencias de software desde la perspectiva del usuario final. *Revista Pilquen*, (7), 0-0.
- Cascón, F. C. (2010). Creación, edición y lectura en la sociedad de la información: entre la propiedad intelectual y el acceso a la cultura. *Pliegos de Yuste: revista de cultura y pensamiento europeos*, (11), 127-134.
- Conde-Gutiérrez, L. A. (2004). La protección jurídica del software. *Revista de Propiedad Intelectual*, (8), 9-26.
- Configegal. (2017, 1 de junio). Dos empresas multadas con 385.462 euros por usar software sin licencia.
- Culebro Juárez, M., Gómez Herrera, W. G., & Torres Sánchez, S. (2006). Software libre vs software propietario. Ventajas y desventajas. *Creative Commons, México*.
- Estrada, O. L. T. (2020). El software, un bien intangible con naturaleza propia. *Dos mil tres mil*, 22, 1-20.
- Fernández-Novoa, C. (2005). Propiedad intelectual en el software. *Anuario Jurídico y Económico Escurialense*, 38, 393-418.
- Free Software Foundation. (s.f.). Categorías de software.
- Gómez Chaves, J. D. (2017). Las patentes de software: un análisis de su estructura y su aplicación.
- López-Noriega, I. (2010). Propiedad intelectual y software: la protección de las creaciones informáticas. *Cuadernos de la Facultad de Derecho*, (20), 123-142.
- Monografías. (s.f.). Tipos de licencias de software.
- Muñoz Machado, S. (2017). Plagiadores, piratas y otros depredadores de la propiedad intelectual. In *ANALES DE LA REAL ACADEMIA DE CIENCIAS MORALES Y POLÍTICAS* (pp. 231-262). Ministerio de Justicia.
- Naldi, G. (2011). Propiedad intelectual y software: alcances y limitaciones del derecho de autor en programas de ordenador. *Ius et Praxis*, 17(1), 167-199.

Núñez, A. (2012). Protección jurídica del software. *Revista Electrónica de Derecho Informático*, 10(1), 1-10.