VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento de Derecho Público General

Área de conocimiento: Derecho Penal

Curso 2016/2017

DERECHO PENAL Y LAS NUEVAS TECNOLOGÍAS

Estudiante: Álvaro Álvarez Pardo

Tutor: Fernando Pérez Álvarez

Julio 2017

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento Derecho Público General

Área de conocimiento Derecho Penal

DERECHO PENAL Y LAS NUEVAS TECNOLOGÍAS.

CRIMINAL LAW AND NEW TECHNOLOGIES.

Nombre del/la estudiante:
ÁLVARO ÁLVAREZ PARDO
e-mail del/a estudiante:
aalvarezp92@alumno.usal.es
Tutor/a: FERNANDO PÉREZ ÁLVAREZ

RESUMEN

Las nuevas tecnologías suponen una forma más sencilla de ejercer nuestros derechos de libertad de expresión o de libertad de información, entre otros. Pero a su vez, también facilitan la labor de los delincuentes para llevar a cabo las conductas que ponen en peligro otros derechos, como la propia imagen, la intimidad, el honor y la protección de los datos personales. Dada la concienciación de este tipo de peligros, se da una mayor demanda de mecanismos que ofrezcan tutela a sus derechos fundamentales.

Por ello, se cuenta con el derecho al olvido, a través del cual se ejerce el derecho de cancelación y oposición en lo que se refiere a los datos personales, en relación con las paginas web y los motores de búsqueda en internet. Este derecho debe ejercitarse respetando otros derechos fundamentales, para que haya una armonización en los intereses de la sociedad.

PALABRAS CLAVE:

Derecho a la protección de datos personales; Internet; nuevas tecnologías; derecho al olvido; motores de búsqueda; delitos informáticos; dirección IP.

ABSTRACT

New technologies are an easer way of exercising our rights to freedom of expression or freedom of information, among others. But at the same time, it also facilitates the work of criminals to carry out behaviors that endanger other rights, such as self image, privacy, honor and protection of personal data. Given the awareness of these types of dangers, there is a greater demand for mechanisms that offer protection to their fundamental rights.

That is why the right to forget is important, through which the right of cancellation and opposition is exercised at personal data, in relation to web pages and search engines on the internet. This right must be exercised with respect for other fundamental rights, so that there is a harmonization in the interests of society.

KEYWORDS:

Right to personal data protection; Internet; new technologies; Right to be forgotten; Search engines; cybercrime; IP address.

ÍNDICE.

INDICE ABREVIATURAS.

AEDP: Agencia Española de Protección de Datos.

Art/s.: artículo/s.

CE: Constitución española de 1978.

INTERPOL: La Organización Internacional de Policía Criminal.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos.

LOPJ: Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

LSSICE: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

ODILA: Observatorio de Delitos Informáticos de Latinoamérica.

STC: Sentencia del Tribunal Constitucional.

SSTC: Sentencias del Tribunal Constitucional.

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos.

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

TC: Tribunal Constitucional.

TJUE: Tribunal de Justicia de la Unión Europea.

TS: Tribunal Supremo.

UE: Unión Europea.

1. INTRODUCCIÓN.

Comprendemos el Derecho penal como aquella rama del Derecho Público encargada de regular la potestad Punitiva del Estado. Esta labor que es llevada a cabo mediante la asociación de hechos, regulados fehacientemente por la ley, a una pena o medida de seguridad, como consecuencia jurídica establecida igualmente por ley. El derecho penal es un termino que abarca varios significados, pudiendo hablar tanto de derecho penal sustantivo (está constituido por lo que generalmente se conoce como código penal o leyes penales de fondo, que son las normas promulgadas por el Estado, que establecen los delitos y las penas), como de derecho penal adjetivo o procesal (mientras que el derecho procesal penal es el conjunto de normas destinadas a establecer el modo de aplicación de las mismas).

Las nuevas tecnologías, algo presente en nuestro tiempo, han llevado a situaciones nuevas que no serian posible sin las nuevas tecnologías. Pero no solo eso sino que algunas conductas que ya eran delito antes de la llegada de las mismas, como el fraude o la estafa, con las nuevas tecnologías han visto una nueva forma de llevarse a cabo. Internet, es un arma de doble filo: pese a aportar grandes beneficios, también tiene su parte oscura, ya que facilita la comisión de innumerables delitos.

A lo largo de este trabajo intentaremos dar sentido y solución a cuestiones que han traído de cabeza al derecho penal con relación a los delitos cometidos a través de las nuevas tecnologías, en especial los realizados mediante el uso de internet. Delimitando como poder perseguir a los delincuentes cuando se encuentren en lugar distinto al de producción del daño, que norma aplicar en conflicto de que haya varios países o territorios involucrados, etc…

Un tema muy extenso, con mil recovecos, por lo que, pese a un análisis general, el punto central de este trabajo, será el Derecho al olvido, cuestión importante y de actualidad social que exige un tratamiento jurídico detenido.

El derecho a olvido ha supuesto muchas controversias, desde sus inicios, entrando siempre en cuestiones sobre afección y conflicto con otros derechos (honor, intimidad, integridad moral…).

2. LAS NUEVAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACION (TICs) Y LA AFECCIÓN A DETERMINADOS BIENES JURÍDICOS DIGNOS DE PROTECCIÓN PENAL.

2.1. DIMENSIÓN DEL PROBLEMA.

El derecho, debe estar dotado de flexibilidad (dentro de sus posibilidades), ya que en los tiempos que corren, surgen cada vez más y más formas de vulnerarlo, por ello debe adaptarse a los cambios y a las nuevas apariciones, dando siempre una seguridad a la sociedad.

El s.XXI ha supuesto la aparición de nuevas tecnologías, y su aplicación e incursión en todos los ámbitos, entre los que incluimos al derecho. Por ello es necesario una adaptación de los profesionales del derecho a la introducción de las nuevas tecnologías en sus hábitos profesionales.
Podemos referirnos a las nuevas tecnologías como una serie de medios cuyo margen oscila desde los hipertextos, los multimedias, Internet, la realidad virtual, o la televisión por satélite. Una característica común que las definen es que giran de manera interactiva en torno a las telecomunicaciones, la informática y los audiovisuales y su combinación como son los multimedias.
Las nuevas tecnologías suponen una gran revolución en lo referente a la sociedad, y por lo tanto en lo referente a sus derechos y a la forma en la cual los mismos pueden ser vulnerados y atacados.
A día de hoy es descomunal la cantidad de información a la que tenemos acceso, la cual además se multiplica a cada instante, siendo necesarias medidas que nos permitan filtrar esa información, en base a las necesidades de cada sujeto.

La información a la que tenemos la puerta abierta, es tan beneficiosa, como peligrosa, por ello es necesario que el derecho penal tome medidas en el asunto, y se procure la preparación de los profesionales del sector en cuanto a esta materia se refiere, desde abogados y jueces, hasta periodistas y ciudadanos.

Internet ha posibilitado que los ciudadanos de a pie tengan un acceso "prácticamente inmediato" a la información, incluyendo en este concepto tan general, a la información jurídica. Pero también ha posibilitado a los delincuentes una nueva forma de llevar a cabo actuaciones que atentan contra los derechos de los ciudadanos, poniendo en peligro numerosos bienes jurídicos, siendo alguno de los contextos más destacados propios de tal delincuencia los siguientes:

- Delitos informáticos: consistentes en la realización de conductas u operaciones por medio de internet consistentes en el engaño a un usuario que se encuentra comprando tranquilamente en la red a través de su ordenador, no siempre se produce el engaño, pero sí en ocasiones. Conductas

consistentes en la oferta de empleo, para que se faciliten datos personales, venta de productos inexistentes, solicitudes de cambio de cuenta corriente, etc… Estos delitos los encontramos tipificados en los artículos 248 a 251 del CP[1].

- Delitos de pedofilia y pornografía infantil: la llegada de las nuevas tecnologías han supuesto una lanzadera, un fácil medio de distribución de este material ilegal, puesto que las imágenes, videos y demás materiales circulan con gran facilidad. Se encuentra regulado en el art. 188 CP[2].
- Delitos realizados por hackers: el hackeo consiste en entrar de forma abrupta y sin permiso a un sistema de cómputo o a una red, obteniendo con esta conducta, archivos, documentos, imágenes, y todo tipo de información de propiedad privada de las personas. Generalmente vulneran la normativa de propiedad intelectual, suponiendo un ataque a quienes son titulares de este derecho.
- Delitos realizados por crackers: aquí la conducta consiste en la introducción en sistemas informáticos remotos, con intención de destruir datos, bloquear el acceso a usuarios legales y

---

[1] Art. 248 CP: **1.** Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

[2] Art. 188 CP: **1.** El que induzca, promueva, favorezca o facilite la prostitución de un menor de edad o una persona con discapacidad necesitada de especial protección, o se lucre con ello, o explote de algún otro modo a un menor o a una persona con discapacidad para estos fines, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses.

Si la víctima fuera menor de dieciséis años, se impondrá la pena de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

2. Si los hechos descritos en el apartado anterior se cometieran con violencia o intimidación, además de las penas de multa previstas, se impondrá la pena de prisión de cinco a diez años si la víctima es menor de dieciséis años, y la pena de prisión de cuatro a seis años en los demás casos.

3. Se impondrán las penas superiores en grado a las previstas en los apartados anteriores, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:

a) Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad, discapacidad o situación.
b) Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, descendiente o hermano, por naturaleza o adopción, o afines, con la víctima.
c) Cuando, para la ejecución del delito, el responsable se hubiera prevalido de su condición de autoridad, agente de ésta o funcionario público. En este caso se impondrá, además, una pena de inhabilitación absoluta de seis a doce años.
d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.
e) Cuando los hechos se hubieren cometido por la actuación conjunta de dos o más personas.
f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

4. El que solicite, acepte u obtenga, a cambio de una remuneración o promesa, una relación sexual con una persona menor de edad o una persona con discapacidad necesitada de especial protección, será castigado con una pena de uno a cuatro años de prisión. Si el menor no hubiera cumplido dieciséis años de edad, se impondrá una pena de dos a seis años de prisión.

5. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las infracciones contra la libertad o indemnidad sexual cometidas sobre los menores y personas con discapacidad necesitadas de especial protección.

legítimos, provocar daños, realizar robos, o incluso provocar perjuicios en beneficio de terceros. Su actuación más habitual es la entrada en bases de datos restringidas para vender la información en ella obtenida, al mejor postor, o quien le contrate con tal fin.

- Delitos de acoso: el Código Penal lo recoge en su art. 172 ter[3], también conocido como "stalking", quedando así tipificado, incluso cuando es ejercitado en su modalidad a través de las nuevas tecnologías. Lo que se busca es penar las alteraciones que se sufren en la vida cotidiana tales como obligando a realizar algo o a dejar de hacerlo (como prohibir ir a un lugar), obligar a cambiar de teléfono, etc… siendo un delito que no es de coacción ni amenaza pero que ya ha sido incluido. Además, del acoso de violencia de género, esto permite perseguir el acoso vecinal o el acoso que sufren personas por el fenómeno fan. Esto está tipificado ya.

A pesar de todas las medidas que hay para luchar contra estos delitos, la mejor medida que se puede tomar no es otro que la formación de la persona para evitarlos, teniendo unos conocimientos, unas pautas y unos filtros, estos delitos pueden verse mermados, aunque no erradicados.

Pese a encontrar diversos medios a través de los cuales se pueden llevar a cabo conductas dañosas, como pueden ser [4]redes sociales (whatsApp, instagram, twitter, facebook…), correos electrónicos, teléfonos móviles, u otros medios, los asociamos todos al uso de internet, ya que es el principal medio de las nuevas tecnologías.

---

[3] Art. 172 ser CP: 1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

[4]Una Red Social es una estructura social integrada por personas, organizaciones o entidades que se encuentran conectadas entre sí por una o varios tipos de relaciones como ser: relaciones de amistad, parentesco, económicas, relaciones sexuales, intereses comunes, experimentación de las mismas creencias, entre otras posibilidades.

Algunos ejemplos de dichas conductas[5] los encontramos por ejemplo en EEUU, donde cabe reseñar *"un ataque masivo por parte de varios hackers y piratas informáticos chinos contra la página Web de la Casa Blanca, entre otros 300 sitios gubernamentales; En la sede de Interpol, sita en Lyón (Francia), su Secretario General, Ronald K. Noble, ha declarado que esta organización está particularmente interesada en la lucha contra la difusión malintencionada de virus, porque se trata de un delito verdaderamente transfronterizo que exige una respuesta de alcance auténticamente mundial y la colaboración a escala mundial entre la policía y las empresas privadas. El Sr. Noble ha añadido que este programa de recompensas de Microsoft brinda la oportunidad de seguir forjando relaciones fructíferas entre las fuerzas policiales de todo el mundo y el sector privado a fin de prevenir la ciber-delincuencia y enjuiciar a sus autores."*

Dicha entidad conocida como la INTERPOL[6] es uno de los principales activistas contra la ciber-delincuencia, luchando contra la misma desde hace más de quince años, en los 181 países miembros de la misma. Uno de sus principales intereses es concertar con el sector privado para la lucha de la ciber-delincuencia y la propagación de virus a través de internet. Comprende un "sistema de alerta rápida" el cual le permite a las distintas fuerzas policiales una comunicación entre ellos, de forma directa, en tiempo real, a través de los mensajes sobre delitos informáticos[7].

Más datos relativos a la materias son los proporcionados por el Estudio Anual sobre Piratería de Programas Informáticos. *"Datos del último estudio IPR, con el 67% Europa Occidental fue la región del planeta con el índice más elevado de piratería. América Latina se situó en segundo lugar con un 57%, por encima de Oriente Medio y África con 52% y Asia-Pacífico con 54%. España es el segundo país de Europa Occidental con mayor índice de delito informático, siendo solo superado por Grecia, el 49% del software que se utilizó en España durante el año 2001/2002 tuvo un origen ilegal, lo que se traduce en unas pérdidas de más de 113 millones de euros para la industria tecnológica del software"*[8].

Respecto a los delitos relacionados con la pornografía infantil, según la Fundación Alia2, en base a un informe sociológico realizado por dicha fundación, en nuestro país, durante el año 2010 más de

[5] Fuente: http://www.tuabogadodefensor.com/derecho-de-nuevas-tecnologias-2/

[6] La Organización Internacional de Policía Criminal, es la mayor organización de policía internacional, con 190 países miembros, por lo cual es una de las organizaciones internacionales más grande del mundo, tan sólo por detrás de las Naciones Unidas. Creada en 1923 bajo el nombre de Comisión Internacional de Policía Criminal, tomó el nombre común de INTERPOL a partir de su dirección telegráfica.
La misión de INTERPOL es la comunicación policial para un mundo más seguro y por eso apoya y ayuda a todas las organizaciones, autoridades y servicios cuyo objetivo es prevenir o combatir la delincuencia internacional.

[7] Todo aquel delito que tenga como acción y/o como instrumento del delito a los sistemas informáticos o a los datos que lo contengan.

[8] Fuente: http://www.tuabogadodefensor.com/derecho-de-nuevas-tecnologias-2/

16.000 personas intercambiaron archivos de contenido pornográfico en el que aparecían menores. Estando por delante solo EEUU.

2.2. ESTADÍSTICAS DE DELITOS (CIFRA OSCURA).

Podemos definir la cifra oscura como aquel número correspondiente a los delincuentes y a los delitos que no han sido condenados o si quiera descubiertos, es aquella cifra que escapa de las estadísticas habituales, bien porque la víctima no sabe dónde o cómo denunciarlas o simplemente porque no realizan la denuncia. Motivo por el cual muchos de estos delitos no salen a la luz.

En internet, hay, por parte de los usuarios, una tendencia a que en internet se puede hacer de todo, habiendo una regulación menos exhaustiva que en otros ámbitos. Esto, obviamente, es falso, ya que existe una legislación en cada país que recoge y regula el tema.

Hay algunas Agencias como la Agencia Española de Protección de datos, la INTERPOL, ODILA, etc… que se encargan de la tutela de los individuos para facilitar la denuncia de tales delitos.

2.3. IDENTIFICACION DE LOS BIENES JURIDICOS.

Podemos definir el bien jurídico, desde el punto de vista del derecho penal, como aquel bien que se protege. Posee carácter jurídico, puesto que existe una norma jurídica que le atribuye una sanción en caso de que dicho bien pueda ser lesionado o perjudicado. Si no existe norma que lo ampare, no constituye carácter jurídico. El bien jurídico adquiere su mayor ponencia en el derecho penal, puesto que el contenido de la ley penal reprime las conductas que atenten contra esos bienes, siempre que estén tuteladas por la ley, de forma inmediata.

De conjunción con el tema abordado, diremos que el bien jurídico, en los delitos informáticos, pueden ser la propiedad, el honor, libertad o indemnidad sexual, etc… Pero como sabemos las nuevas tecnologías van más allá de los delitos informáticos, por lo que el uso de las mismas sirven para alcanzar otro u otros objetivos, pueden vulnerarse otros bines jurídicos, como pueden ser la salud, el patrimonio, intimidad, honor, dignidad, etc…

Estas nuevas tecnologías hacen más fáciles la comisión de delitos, facilitan la puesta en relación de manera más sencilla, la obtenciones de materiales necesarios para llevar a cabo las conductas. Debiendo matizar en este asunto, que es la ingeniería técnica o social que se utiliza la que debe criminalizarse, y no los medios, es decir, debe castigarse la conducta realizada para llevar a cabo el delito, y no los medios técnicos (teléfono móvil, ordenador…) utilizados para llevarlo a cabo.

2.3.1. DERECHO AL HONOR, INTIMIDAD Y LA PROPIA IMAGEN.

Un tema importante, es la vida privada, y la "des-privación" de esta privacidad, debido a la negligente gestión que hacemos de nuestra intimidad, ya que el ámbito online nos ha llevado a una administración irresponsable de la misma, siendo necesario, más que nunca, una concienciación social sobre el asunto, con prioridad en los menores de edad, sobre la gestión, custodia, control y difusión de su privacidad[9].

En torno a la vida privada, y los derechos al honor, la intimidad y la propia imagen, encontramos su regulación en los artículos 197 y ss CP[10].

Las redes sociales son los principales promotores de esta negligente administración personal, la divulgación masiva de imágenes, sobre todo ahora con los llamados "selfies"[11] y las fotos temporales de las principales redes sociales, en especial instagram. Algo habitual a día de hoy, pero inimaginable hace 20 años.

La sociedad ha normalizado esta difusión masiva de información intima, personal, siendo los grandes perjudicados los menores (y/o adolescentes), puesto que la influencia social les lleva a emisiones de sus fotos o videos, de situaciones intimas, de forma voluntaria y consciente, y de forma instantánea, por no decir coetánea a su celebración.

La aparición de la LOPD de 1999/32[12], diferencia el derecho de protección de datos, o de autodeterminación informativa delimitándolo del derecho a la intimidad.

Para constatar y reforzar lo anteriormente dicho, nos vamos a apoyar en la STC 30 noviembre 2000/33, que supone una construcción jurisprudencial del derecho a la protección de datos o

---

[9] 30 V. De la Torre Olid, F./Conde Colmenero, P.:"Consideraciones críticas en torno a la autogestión y preservación de la intimidad en un escenario de riesgo", en AA.VV.: *Los derechos a la intimidad y a la privacidad en el siglo XXI* (coord. por A. FAyos gArdó), Dykinson, Madrid, 1a ed., 2015, p. 41.

[10] Art. 197 CP: **1.** El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

[11] Es un autorretrato realizado con una cámara fotográfica, típicamente una cámara digital o teléfono móvil. Se trata de una práctica muy asociada a las redes sociales, ya que es común subir este tipo de autorretratos a dichas plataformas.

[12] Ley Orgánica de Protección de Datos de carácter personal.

autodeterminación informativa, como derecho fundamental autónomo que "garantiza a las personas un poder de control respecto al uso y destino de sus datos"[13].

2.3.2 DERECHO A LA PROPIEDAD INTELECTUAL.

El contexto más conocido en este ámbito es el de piratería, siendo normalmente la conducta realizada para la obtención de material que corresponde a ciertos autores, suponiendo una vulneración de los derechos de autor u otros derechos afines de carácter comercial. Es la conducta lesiva más practicada en nuestro tiempo, en lo referido a la propiedad intelectual.

Dada su repercusión, no se ha tardado en tomar medidas al respecto, en primer lugar encontramos la propia Ley de Propiedad Intelectual[14], pero al margen de esta vamos a destacar otras cuatro medidas para su protección:

1) Comisión interministerial para actuar contra las actividades vulneradoras de la propiedad intelectual e industrial, aprobada por el RD 114/2000 , de 28 de enero. Se justificó por la necesidad de coordinación de las políticas públicas para la lucha contra la piratería.
2) Plan integral del Gobierno para la disminución y eliminación de las actividades vulneradoras de la propiedad intelectual. Consta de una serie de medidas para dirigidas a analizar la piratería en sus diversas pendientes.
3) Ley 23/2006, de 7 de julio[15], siendo su principal aportación el llamado canon[16], permitiendo así recibir una remuneración el titular de los derechos de autor a modo de compensación por la realización de copias privadas.
4) Ley Sinde[17], hasta ahora, la actuación mas contundente frente a la lesión de los derechos de autor, posibilitando el cierre de paginas webs que vulneren los derechos de autor, con intervención judicial.

Obviamente estas conductas de acceso y distribución de obras protegidas se ha reforzado por la evolución tecnológica experimentada en los últimos años. Internet ha supuesto una medida que facilita la transmisión, distribución y comunicación entre miles de millones de usuarios, con todos los beneficios que ello supone, pero también dando facilidad a quienes lo utilizan con fines tipificados y prohibidos.

---

[13] Cfr. Simón Castellano, P.: El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras las sentencia del TJUE de mayo de 2014, cit., p.186.

[14] 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.

[15] Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

[16] Compensación por copia privada.

[17] Disposición incluida en la Ley de Economía Sostenible (Ley 2/2011 de 4 de marzo).

La respuesta legal la encontramos en la ya citada Ley de Propiedad Intelectual, pero desde la perspectiva del derecho penal, debemos acudir a su art. 270[18], que exige entre otros requisitos el animo de lucro del autor y que sea en perjuicio de un tercero.

2.3.3. DERECHO DE LIBERTAD E INDEMNIDAD SEXUAL.

La aparición de internet a finales del pasado siglo, multiplico exponencialmente la transferencia, distribución y posesión de material perjudicial en materia de indemnidad sexual, y sobre todo en materia de indemnidad sexual en materia infantil.

Podemos definir estos delitos como los que promueven la sexualidad en alguna faceta cuando el sujeto en cuestión no llega a la mayoría de edad de consentimiento estipulada por la ley o cuando el sujeto mayor de sedando consiente en la vulneración de su libertad en el planos sexual. Están incluidos el acoso sexual, la agresión sexual, el abuso sexual, el exhibicionismo, la provocación sexual y la corrupción de menores.

El enorme aumento de conductas típicas en la materia, y el crecimiento de los medios tecnológicos para llevar a cabo estas conductas tipificas en la ley, han hecho que se motiven de forma fehaciente continuas y numerosas iniciativas internacionales para paliar el problema[19].

---

[18] Art 270 CP: **1.** Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.
3. En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.
Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.

[19] Puede verse un elenco completo en MORILLAS FERNANDEZ, D. L., Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comitivas con internet, Dykinson, Madrid, 2005, p. 480-481.

Destacando entre ellas, en un primer lugar, la Convención sobre Derechos del Niño, en la se obligaba a sus países miembros, firmantes y que hayan ratificado el adoptar las medidas necesarias para proteger a los niños de lo peligros que pudiesen sufrir, por sus padres u otras personas; en segundo lugar, la celebración de los Congresos Mundiales contra la Explotación Sexual Comercial de los Niños[20].

Por otra parte, el Consejo Europeo de Viena (diciembre 1998) solicitó a escala internacional y europea las iniciativas para la protección de la indemnidad sexual de menores, con énfasis en el ámbito de la pornografía de menores en internet.

Por ultimo, en el caso de nuestro país, el tema en cuestión tuvo tanta transcendencia que se procedió a una [21]reforma expansiva en lo que a delitos de ámbito sexual relacionado con menores se trata. Dicha reforma supuso un endurecimiento, reforzado a su con posteriores reformas[22].
Encontramos la sanción penal en aquellos supuestos de los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores en los [23]artículos del CP, del 187 al 189.

3. LAS DIFICULTADES DE NEUTRALIZAR O PALIAR LOS RIESGOS DE LOS DELITOS COMETIDOS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS.

Como hemos citado en apartados anteriores, el descomunal aumento y expansión que ha sufrido internet en estos años, a la par que el aumento masivo de información, ha supuesto la adopción de internet como principal actor en todo tipo de actividades (lúdicas, culturales, financieras, comerciales…).

Pero por supuesto este crecimiento ha sido en un doble sentido, porque a su vez ha provocado un elevado numero de actividades lesivas para la sociedad y para los ciudadanos, suponiendo daños en bienes jurídicos importantes. De forma general, las conductas han supuesto una actualización de delitos ya tipificados por nuestro Código Penal, pero apoyados esos delitos en estas nuevas

[20] El primero se celebró en Estocolmo en 1996 y el segundo en Yokohama, Japón, en diciembre de 2001.
[21] Ley Orgánica 11/1999, de 30 de abril.
[22] Ley Orgánica 15/2003 de 25 de noviembre y Ley Orgánica 5/2010 (incluyó el child grooming).
[23] Art. 187 CP trata sobre la violación de menores. Art. 188 CP trata la prostitución de menores de edad. Art. 189 CP trata la distribución y posesión de pornografía infantil.

tecnologías[24]. Hay que aclarar que no todas las conductas son una nueva versión de conductas ya tipificadas, sino que también nos vamos a encontrar con un catálogo de conductas nuevas, basadas en las nuevas tecnologías y su uso para llevarlas a cabo.

Encontramos defectos estructurales debidos a la construcción de los tipos penales, además de otra serie de factores que obstaculizan la lucha contra la criminalidad a través de los nuevos medios, factores que dificultan la determinación y persecución de los delitos cometidos a través de internet, por ello el éxito de los delitos así cometidos.

El problema que encontramos en esta materia, visto de forma unitaria, es el problema de persecución (como principal y mayor problema), dado que no siempre resulta fácil encontrar al autor o autores del delito. Este problema podemos dividirlo en dos: el anonimato y los delitos a distancia y la competencia territorial.

3.1. PROBLEMAS DE PERSECUCIÓN (I): ANONIMATO: LA LEY 25/2007, DE 18 DE OCTUBRE, DE CONSERVACION DE LOS DATOS RELATIVOS A LAS COMUNICACIONES Y A LAS REDES PÚBLICAS DE COMUNICACIÓN.

Detectar al autor de un delito cometido a través de internet puede ser difícil y pedregoso. Cuando un dispositivo electrónico (ordenador, móvil…) se conecta a internet, tiene asignada una dirección IP[25]. En principio no es difícil su seguimiento y detección, aunque se trate de un IP dinámico. Sin embargo, los medios permiten modificar esa dirección IP, haciendo difícil garantizar la determinación de la dirección del emisor.

El proceso para la identificación del emisor, consiste en que una vez dispongamos de la IP se solicita al juzgado, para que este se dirija a los proveedores de internet para que estos ayuden mediante los datos que posean para proceder a su identificación. Posteriormente, mediante auto del tribunal, se lleva a cabo la diligencia de entrada y registro del domicilio que coincida con la dirección IP asemejada al delito, pudiendo mediante presencia y levantamiento de acta de un secretario judicial acceder al dispositivo y sus archivos para obtener copia.

[24] Una visión general en CORCOY BIDASOLO, M., <<Problematica de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y el ámbito espacio-temporal de comisión de los hechos>>, en Egukilore, núm. 21, diciembre 2007, pp. 7 y ss.

[25] TCP/IP (Transmision Control Protocol/Internet Protocol): familia de protocolos que hacen posible la interconexión y trafico de red en internet.

En un primer momento, este proceso de identificación no era sencillo (incluso en ocasiones a día de hoy no lo sigue siendo), por falta de medios y por ser algo nuevo del que se poseía muy poca información. La LSSI[26]reforzó los medios de identificación de las direcciones IP, imponiendo a algunos prestadores de servicios la obligación de cumplir una serie de exigencias en sus actuaciones que sirvieran a los órganos judiciales para dicha identificación. Esta LSSI fue suplida por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunidades electrónicas y a las redes públicas de comunicaciones.

La directiva 2006/24/CE, del Parlamento Europeo y del Consejo. de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones, fue transpuesta a nuestro ordenamiento, incluyendo por lo tanto dicha norma en nuestra ley. Esta directiva le obliga a operadores de telecomunicaciones a guardar datos que se generan, para poder acudir a ellos los agentes que posean legitimación para ello.

Lo que sacamos en común, es que para conocer al titular de la dirección IP, es necesario conocer previamente la misma. Por esta razón surgen las dudas de la posible vulneración del art. [27]18.1 y 18.3 CE, en los que se garantiza el secreto de las comunicaciones en los casos en que la policía inicia una investigación cuando hay denuncia por parte de un tercero, consiguiendo la dirección IP del acusado por medios extrajudiciales.

Respecto a este tema, es bastante esclarecedor atender a la STS de 12 de noviembre de 2008 y las que se recogen en la misma, referente al tema de los rastreos que realiza la policía judicial. Dando una respuesta negativa al tema de la vulneración de derechos.

Otras sentencias a tener en cuenta[28] son:

- STS de 9 mayo de 2008 (RJ 2008, 4648): *<<a) los rastreos que realiza el equipo de delitos telepáticos de la guardia civil en internet tienen por objeto desenmascarar la identidad critica de los IPS (internet protocols) que habían accedido a los hush que contenían pornografia infantil. el acceso a dicha información, calificada como de ilegitima o irregular, pueden*

[26] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónicos, Ley 34/2002, de 11 de julio.

[27] Art. 18.1 CE: Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
Art. 18.3 CE: Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

[28] Fuente: Fernández Teruel, J. G. <<Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescentes>>

efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre, y ello lo sabe el usuario. b) Entender que conforme a la legalidad antes citada (…) se hace preciso, sin embargo, acudir a la autorización del juez instructor, para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data). Consecuentemente quien utiliza un programa P2P, en nuestro caso EMULE, asume que mucho de los datos se convierten en publico para los usuarios de internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos publicados en internet, no se hallaban protegidos por art. 18.1. y 18.3 de la CE>>

- STS de 7 de octubre de 2010 (RJ 2010/7684): << *la jurisprudencia de esta Sala, entre otras la STS núm. 739/2008, de 12 de noviembre (RJ 2009, 167) y las que en ellas se citan, y la STS núm. 680/2010 (RJ 2010, 3509), que cita la anterior, ha señalado que en esta materia de debe concluir, en primer lugar, que los rastreos que realizan en estos casos los agentes policiales tienen por objeto desenmascarar la identidad críptica de los IPS (internet protocols) que había accedido a los hush que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización policial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre y ello lo debe al usuario. Y, en segundo lugar, que, de acuerdo con la legalidad citada en la referidas sentencias, se hace preciso, sin embargo, acudir a la autorización del juez instructor para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data). Consecuentemente quien utiliza un programa P2P asume que mucho de los datos que el mismo incorpora a la red cónsul actividad se convierten en publico para los usuarios de internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos publicados en internet, no se hallaban protegidos por art. 18.1. y 18.3 de la CE, por lo que no era precisa la autorización judicial para obtener las identificaciones de las IPs involucradas en las descargas de archivo de contenido pedófilo.*

Hay que señalar que la IP en algunos casos, posee un carácter público, pero que es limitado a los interlocutores, impidiendo, al menos al principio, el acceso a la misma de terceros. Solo conocen la IP las dos partes que establecen la conexión. Puede darse la situación de que una de las partes

comparta esa dirección IP, afectando a la intimidad, pero no es algo a lo que los terceros tengan libre accesibilidad.

3.2. PROBLEMAS DE PERSECUCIÓN (II): DELITOS A DISTANCIA Y COMPETENCIA TERRITORIAL.

En lo referente a los delitos, por regla general, entendemos que la comisión del delito se produce en el lugar donde se realiza el delito, es lo que conocemos como como lugar del delito que es importante para al aplicación del principio de territorialidad[29] como principio fundamental en la determinación de la jurisdicción aplicable para el delincuente o delincuentes implicados. Este principio resulta poco compatible con los delitos cometidos en internet o por medio de nuevas tecnologías, debido a que la conducta delictiva puede tener su origen en uno o varios países, produciéndose finalmente en otro u otros distintos. En España, la regla de la territorialidad la encontramos en el art. 23.1[30] LOPJ, existiendo excepciones a este citado principio, en base a los principios de personalidad del delincuente, real o de protección de intereses y de justicia universal, recogidos a lo largo de este art. 23 LOPJ.

A día de hoy en la indagación de cual sea el lugar de la comisión del delito, nos encontramos con tres posibles soluciones, plasmados a modo de teorías: 1)Teoría de la actividad, donde se produce la el delito de forma externa es donde se entiende cometido; 2)Teoría del resultado, donde se produce el resultado externo, es donde se produce el delito; 3)Teoría de la ubicuidad, entiende que el delito se cometió en el lugar en el que se lleva a cabo la actividad o se manifiesta el resultado.

La doctrina se ha visto más próxima a la teoría del resultado, pero esta no siempre es válida (sobre todo en delitos a distancia, siendo mejor en estos casos acudir a la teoría de la ubicuidad). El TS ya ha admitido esta posibilidad, entendiendo el resultado y la acción como elementos del tipo, siendo el lugar de comisión aquel en que coincidan ambos, así lo dicta el auto de 20 de mayo de 1992 (RJ 1992/4195): <<*Sin embargo, cuando la acción y el resultado no tengan lugar dentro de una misma*

[29] El principio de territorialidad puede definirse como aquél criterio que establece la aplicación con carácter exclusivo de la ley penal del territorio a todos los hechos delictivos que se cometen en el mismo.
En correspondencia con esta afirmación es indudable que el significado genuino de este principio deriva precisamente, de la estimación del territorio como espacio en que la ley penal de un Estado halla su ámbito de aplicación. Y, ciertamente, de este modo es posible señalar un significado positivo, coincidente con lo anterior, puesto que un Estado puede someter a su poder punitivo todas aquellas acciones que se cometan en su territorio, y otro negativo, en cuanto la consecuencia que produce la aplicación exclusiva de la ley penal nacional en ese territorio es la ausencia de la aplicación de la misma a hechos ocurridos más allá de esos límites, y asimismo, la negativa a la aplicación de la ley penal extranjera.

[30] Art. 23.1 LOPJ: En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte.

jurisdicción, es de aplicación el principio de ubicuidad, según el cual tanto el lugar de acción como el lugar de resultado deben ser relevantes a efectos del art. 14.2 LECrim>>. Siendo frecuente que solo uno de los dos elementos se manifieste en un país.

Otro problema frente al que nos encontramos, son aquellos delitos que no requieren resultado, hablamos de los delitos de simple actividad[31], impidiendo que nos apoyemos en la teoría del resultado. Tal como ocurre con actividades como la difusión de videos o imágenes de contenido pornográfico.

También supone problema cuando el resultado del delito se da en España pero su comisión se ha producido en un país diferente. Chocando en estos casos la pretensión de las autoridades españolas con la pretensión de terceros países de la aplicación de la teoría de la ubicuidad.

En el supuesto de que haya una multitud de afectados por el delito, y estos se encuentren en territorios diferentes, como puede ser el fraude a través de internet, no tienen una regulación con una solución única e inequívoca. Para solucionar dicha situación, acudimos al [32]art. 65.1.c, en relación con el art. 88 LOPJ[33], el cual delega la competencia para conocer el asunto cuando haya una generalidad de personas al Juzgado Central de Instrucción.

La norma general de la jurisprudencia del TS, atiende a la teoría del resultado antes mencionada, por la que el delito se produce donde se consuma, ya que es donde prevalece el perjuicio producido y donde hay una mayor cercanía de las pruebas. De todos modos, cuando no se tiene constancia, o no se conoce el lugar de comisión de dichos delitos, esta regla general plantea excepciones, como advertimos seguidamente.

[31] Los delitos de mera actividad (arts. 15 y 16 del CP) son aquellos cuya descripción y contenido material se agota en la realización de una conducta, sin que se exija la producción de un resultado distinto del comportamiento mismo.

[32] Art. 65.1.c LOPJ: Defraudaciones y maquinaciones para alterar el precio de las cosas que produzcan o puedan producir grave repercusión en la seguridad del tráfico mercantil, en la economía nacional o perjuicio patrimonial en una generalidad de personas en el territorio de más de una Audiencia.

[33] Art. 88 LOPJ: En la villa de Madrid podrá haber uno o más Juzgados Centrales de Instrucción, con jurisdicción en toda España, que instruirán las causas cuyo enjuiciamiento corresponda a la Sala de lo Penal de la Audiencia Nacional o, en su caso, a los Juzgados Centrales de lo Penal y tramitarán los expedientes de ejecución de las órdenes europeas de detención y entrega, los procedimientos de extradición pasiva, los relativos a la emisión y la ejecución de otros instrumentos de reconocimiento mutuo de resoluciones penales en la Unión Europea que les atribuya la ley, así como las solicitudes de información entre los servicios de seguridad de los Estados miembros de la Unión Europea cuando requieran autorización judicial, en los términos previstos en la ley.

AAP Madrid de 14 de mayo de 2009 (ARP 2009/853):

<<En el auto de fecha de 1 de abril de 2009, la juez de Instrucción fundamenta su decisión en que, a tener de las diligencias practicadas, los pagos efectuados por los denunciados tuvieron lugar mediante transferencia bancaria realizada vía internet, desde la pagina ING DIRECT que carece de una sucursal física. (…) Aparentemente no es posible determinar el lugar en el que el delito ha sido cometido. En este caso, entrarían en juego las reglas establecidas en el artículo 15 de la LECrim, conforme a las cuales podrían resultar competentes (lugar de recepción de la transferencia). (…) Es cierto que al haberse autorizadlas transferencias bancarias vea internet y, al menos en el caso del denunciante Sr Saturnino, desde la pagina ING DIRECT, no existe, como informó la Brigada de la Policia Judicial al Juzgado de instrucción, una sucursal física. Pero si es posible que la cuenta ordenan se encuentre asociada o vinculada a una cuenta corriente de otra entidad bancaria que si tenga sucursal, y en ese caso su lugar de ubicación seria el de comisión del delito>>.

En supuestos de este tipo aparecen soluciones dispares. Unas sentencias dicen que será el lugar del domicilio del querellado (Auto AP Madrid de 17 de noviembre de 2003), otras que será donde este ubicada la sede de la empresa desde la que se ejecuta el delito (auto del TS de 22 de julio de 2002), otras del lugar de ubicación del servidor (ATS de 25 de abril de 2005), otras del lugar del descubrimiento de las pruebas materiales (AATS de 3 de abril de 2006 y de 13 de julio de 2006), incluso otras que dicen que en el lugar donde se celebró el contrato (AAP Madrid de 27 de marzo de 2007).

En aquellos casos en los que se vea relación con material pornográfico de carácter infantil, supuestos de difusión, en principio son competentes los juzgados de la sede en que se haya introducido en la red el material pornográfico.

4. EL DERECHO AL OLVIDO EN INTERNET.

4.1.¿QUE ES EL DERECHO AL OLVIDO? DEFINICIÓN.

Samuel D. Warren y Louis D. Brandeis, en Boston en Diciembre de 1890 ya nos advertían *"Que el individuo debería tener protección de su persona y sus propiedades es un principio tan antiguo como la ley, pero de vez en cuando es necesario definir de nuevo la naturaleza y el alcance de esa protección. Cambios políticos, sociales y económicos, suponen el reconocimiento de nuevos derechos, y la Ley, en su eterna juventud, debe crecer para satisfacer las nuevas demandas de la sociedad. Inicialmente la Ley dio remedio a la interferencia física con la vida y la propiedad privada. Más tarde se reconoció la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto de modo que el derecho a la vida se convirtió en el derecho a disfrutar de la vida, – el derecho al olvido, a que te dejen en paz, asegura el ejercicio de los amplios privilegios civiles, y el*

término "propiedad "ha crecido hasta incluir toda forma de posesión – intangible, así como tangible."

Warren y Bramdeis definen la privacidad como el "derecho a que te dejen en paz", o como lo conocemos nosotros, el derecho al olvido.

En los tiempos actuales, cuando hablábamos de los beneficios y de los perjuicios que habían traído las nuevas tecnologías al ámbito de los derechos de las personas, de los bienes de las mismas y de la sociedad en general, hablábamos de medidas a adoptar para el mejor uso de las mismas y un menor perjuicio para los usuarios, entre las que destacamos un derecho reconocido y puesto en nuestra sociedad, el derecho al olvido.

Para Simón Castellano, figura muy representativa de esta materia en España, el derecho al olvido digital podría considerarse *"como un derecho que exige que los datos de las personas dejen de ser accesibles en la web, por petición de las mismas y cuando estas lo decidan; como un derecho a retirarse del sistema y eliminar la información personal que la red contiene. Más concretamente, se trata de un derecho de la ciudadanía a cancelar y oponerse al tratamiento de sus datos personales cuando estos han dejado de ser útiles o necesarios para el propósito con el que fueron recabados o publicados."*

Podemos definir el derecho al olvido como una actualización, una reformulación, de otros derechos como son el de cancelación y oposición, en su uso en los buscadores de internet. Su finalidad, o principal objetivo, es impedir la emisión y/o distribución de la información personal por la red[34], cuando no se reúnen los requisitos de pertinencia y homologación previstos en la normativa, respecto de los datos publicados. Contiene el derecho para poner limites a la emisión (difusión, distribución…) de forma indiscriminada y universal de datos, cuando los mismos son anticuados o irrelevantes, o han dejado de ser de interés público, incluso cuando su publicación se realizó de forma legítima (boletines oficiales o informaciones verídicas).
Según la AGPD, el "*derecho al olvido hace referencia al derecho que tiene un ciudadano a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa".*

[34] Red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.

Relacionamos el derecho al olvido con la protección de datos personales (honor, intimidad e imagen), y también con el Habeas Data[35]. Como mencionaba antes, tiene como función la supresión o bloqueo de información personal que aparece a través de los motores de búsqueda[36], siendo una información verídica, pero anticuada o irrelevante, bien por alteraciones que se haya sufrido, o bien por el mero paso de tiempo. El problema que puede suponer este concepto, es la agresión a la libertad de expresión y a la libertad de información, pudiendo en ocasiones chocar con ellas.

La desmesurada extensión de internet[37], que posee, además de una cantidad de información que resulta casi inimaginable, potentes motores de búsqueda, que conceden el acceso a toda esa información de forma fácil y veloz, suponiendo un obstáculo al derecho al olvido. También hemos de tener presentes la longevidad que rodea a esa información, siendo perenne, suponiendo otro bache al que el derecho debe hacer frente, permitiendo a un sujeto borrar su información, borrar su pasado. El ejercicio de este citado derecho, puede, dirigirse contra el emisor original o medio que lo emitir originalmente, quien publicó los datos, o bien puede haber una acción de este derecho contra los buscadores[38], como veremos.

4.2. RECONOCIMIENTO.

Uno de los principales problemas que presentan los perfiles online, los datos que nuestras cuentas en las redes sociales manejan, o incluso la información a la que es accesible a través de los correos, es cuando pueden ser cesadas dichas fuentes de información, una vez los titulares de las mismas

---

[35] El *habeas data* es una acción jurisdiccional, normalmente constitucional, que puede ejercer cualquier persona física o jurídica, que estuviera incluida en un registro o banco de datos de todo tipo, ya sea en instituciones públicas o privadas, en registros informáticos o no, a fin de que le sea suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad. La frase legal se utiliza en latín, cuya traducción más literal es «tener datos presentes» siendo «hábeās» la segunda persona singular del presente de subjuntivo del verbo latino «habēre» (en este caso entendido como «tener»).
Este derecho se fue expandiendo y comenzó a ser reglamentado tanto por leyes de *habeas data* como por normas de protección de datos personales, que suelen tener un capítulo procesal donde se describe el objeto de la acción de *habeas data*, la legitimación pasiva y activa, y la prueba y la sentencia.

[36] Un motor de búsqueda o buscador es un sistema informático que busca archivos almacenados en servidores web gracias a su *spider* (también llamado araña web).[1] Un ejemplo son los buscadores de Internet (algunos buscan únicamente en la web, pero otros lo hacen además en noticias, servicios como Gopher, FTP, etc.) cuando se pide información sobre algún tema. Las búsquedas se hacen con palabras clave o con árboles jerárquicos por temas; el resultado de la búsqueda «Página de resultados del buscador» es un listado de direcciones web en los que se mencionan temas relacionados con las palabras clave buscadas.

[37] Eric Schmidt, el presidente de Google, afirmó el año pasado que en la red había 5 millones de terabytes de datos. Tomando en cuenta que en un Terabyte caben un millón de libros gruesos, eso quiere decir que en internet podría caber el equivalente a 5 billones de libros.
La universidad de Berkeley dijo una vez que había en internet más palabras que todas las que había pronunciado la humanidad a lo largo de su historia.
Son cálculos hechos al azar porque nadie tiene la varita mágica para ofrecer la cifra más creíble.

[38] El último informe de transparencia de Google se refleja que desde el año 2014 ha recibido 671.463 solicitudes

fallezcan, y es aquí donde cobra importancia "El Derecho al Olvido" siendo el principal actor para solventar los problemas que dichas cuentas y datos puedan suponer.

El TJUE, en mayo de 2014, publicó una sentencia que dictaba que los datos a los que tienen acceso los motores de búsqueda en internet y otros medios, están sometidos a la normativa vigente en la Unión Europea de protección de datos, pudiendo ser solicitados por las personas, respetando, eso si, una serie de requisitos, la desaparición de sus datos personales en relación con los resultados de los motores de búsqueda y esos datos asociados a su nombre, cosa que ya venia diciendo la AEPD en sus resoluciones.

La propia AEPD emitió una nota informativa[39] respecto al asunto, en la cual decía lo siguiente: "*En relación con la sentencia del Tribunal Supremo que clarifica ante quién deben dirigirse las peticiones de 'derecho al olvido', la AEPD recuerda que la forma en la que los ciudadanos pueden ejercer este derecho frente a Google se mantiene intacta.*

La Sala Tercera del Tribunal Supremo ha hecho pública una sentencia en la que clarifica ante quién deben dirigirse las peticiones de 'derecho al olvido'.

La forma en la que los ciudadanos pueden ejercer su 'derecho al olvido' frente a Google se mantiene intacta. Los usuarios pueden seguir dirigiéndose a Google para ello, por ejemplo, a través del formulario que la compañía mantiene habilitado en español desde el 30 de mayo de 2014. La sentencia del TS no tiene por qué afectar a los tiempos de respuesta que ya estaba ofreciendo la compañía. Del mismo modo, si Google deniega la solicitud del interesado o éste no estuviera conforme con la decisión de la compañía, podrá seguir solicitando la tutela de la Agencia en los mismos términos en que podía hacerlo hasta ahora.

En todo caso, es necesario subrayar que la sentencia no supone que los interesados no puedan ejercer sus derechos conforme a lo previsto en la LOPD ni que deje de aplicarse la Ley española. Tampoco modifica los principios y criterios de ponderación que estableció el TJUE en su sentencia, sino que aclara que el destinatario de las solicitudes deberá ser Google Inc.

La Agencia informa de que los ciudadanos afectados directamente por la anulación de las sentencias de la Audiencia Nacional pueden garantizar su derecho del siguiente modo:

- *Comprobando, en primer término, si Google ha vuelto a indexar los enlaces. En caso afirmativo, solicitando el ejercicio de su 'derecho al olvido' a través del formulario que la compañía tiene habilitado.*

[39] Nota informativa de la AEPD con fecha de 15 de marzo de 2016.

- *Si la entidad no responde a la petición realizada o el ciudadano considera que la respuesta que recibe no es la adecuada, puede seguir solicitando la tutela de la Agencia Española de Protección de Datos frente a Google".*

4.3. EL EJERCICIO DEL DERECHO AL OLVIDO.

Para adentrarnos en este apartado, vamos a tener presentes dos sentencias de la Sala de lo Contencioso-Administrativo del TS: sentencias núm. 1381 y 1387/2016, ambas de 13 de junio de 2016. Estas sentencias vienen a consolidar el método a seguir para el correcto ejercicio para el derecho al olvido, tomando como referencia el Reglamento Europeo de Protección de Datos[40].

Las sentencias dicen que *"en el ámbito de esta jurisdicción contencioso-administrativa, la tutela de los derechos de oposición, acceso, rectificación y cancelación reconocidos al titular de los datos personales objeto de tratamiento, se recaba mediante la impugnación de la correspondiente resolución de la Agencia Española de Protección de Datos.*
Este procedimiento comienza con la reclamación o comunicación dirigida al responsable del tratamiento, ejercitando el correspondiente derecho (art. 25 R.D. 1720/2007), frente a cuya respuesta el interesado puede formular reclamación ante la referida Agencia Española de Protección de Datos (art. 117 R.D. 1720/2007), que deberá dictar resolución en el plazo de seis meses, contra la cual puede interponerse el recurso contencioso administrativo (art. 18 LOPD 15/1999)."

Además el TS aclara, que se añade el contenido del citado Reglamento a lo confirmado por sentencias anteriores, tales como la sentencias de 11 de marzo (recursos 643/2015 y 1482/2015), la sentencia de 14 de marzo (recursos 1078/2015 y 1380/2015) y la sentencia15 de marzo de 2016 (recurso 804/2015).

En España, la legislación en vigor, dice que es un requisito imprescindible y fundamental, el hecho de que el sujeto interesado se dirija en primer lugar al buscador (o entidad que se encuentra en posesión y tratamiento de los mismos) para el correcto ejercicio del derecho al olvido. Es cierto que los principales buscadores[41] han facilitado a los usuarios unos formularios, propios de cada uno de ellos de forma particular, para que a través de los mismos se realicen las peticiones para el ejercicio del derecho al olvido.

[40] Reglamento (UE) 2016/679, de 27 de abril de 2016.
[41] Google, Yahoo o Bing.

Puede darse el caso de que la entidad no responda o lo haga de forma que no satisfaga las pretensiones del sujeto interesado, si esto sucede, se puede dirigir a la AEPD para que esta se encargue de tutelar frente al responsable su derecho. Analizando concretamente cada caso, la AEPD le comunicará si estima o no el caso que se le presenta y su es oportuna la tutela del derecho al olvido, siendo la decisión que tome la agencia, respecto a si lo tutela o no, recurriese ante los Tribunales.

4.3.1. EL EJERCICIO DEL DERECHO AL OLVIDO FRENTE A UN BUSCADOR (CON CARACTER PREVIO A LA FUENTE ORIGINAL).

Como vimos anteriormente, se puede ejercer el derecho al olvido frente al buscador, de forma previa a la fuente o emisor original.

Hay diferencia en la forma que tienen los emisores originales en lo relativo a los tratamiento de esos datos, con respecto a los motores de búsqueda. Diferentes en cuanto al ya dicho tratamiento, pero también poseedores de una legitimación diferente y cuyo impacto sobre la privacidad también difiere. Razón por la cual, y con bastante frecuencia de hecho, sucede que se le concede el derecho frente al motor de búsqueda, pero no frente al emisor original, y esto se debe a que el buscador realiza una difusión universal, provocando un impacto que puede perjudicar de forma gravosa a su privacidad e intimidad.

Esto no quiere decir que si nosotros ejercitamos este derecho frente al motor de búsqueda, y se nos concede tal ejercicio, la información sea erradicada de internet. Ya que como dicta la sentencia del TJUE de 13 de mayo de 2014 *"el ejercicio de los derechos de cancelación y oposición realizado frente a los buscadores sólo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona y no implica que la página deba ser suprimida de los índices del buscador ni de la fuente original. El enlace que se muestra en el buscador sólo dejará de ser visible cuando la búsqueda se realice a través del nombre de la persona que ejerció su derecho. Las fuentes permanecen inalteradas y el resultado se seguirá mostrando cuando la búsqueda se realice por cualquier otra palabra o término distinta al nombre del afectado".*

Lo que de aquí sacamos, es que el ejercicio del derecho al olvido, afecta de forma única a los resultados de los buscadores en relación al nombre del sujeto en cuestión, no suponiendo la supresión de la página de la base de datos de los buscadores, ni tampoco de la [42]fuente original. El

[42] Las fuentes originales o primarias contienen información nueva y original, resultado de un trabajo intelectual.

enlace únicamente no estará al alcance de los buscadores cuando se utilice para llegar a esos datos el nombre de la persona que solicito dicho derecho.

4.4. ¿SUPONE EL DERECHO AL OLVIDO UN LIMITE A LA LIBERTAD DE EXPRESIÓN Y A LA LIBERTAD DE INFORMACIÓN?

Tomando como apoyo la anterior sentencia podemos decir que no, no se produce una limitación respecto a la libertad de expresión e información por el ejercicio del derecho al olvido. Como dice la sentencia, es preciso, cuando hablamos de buscadores, una ponderación en cada caso concreto para así pesar las razones y no provocar un desajuste entre los diferentes intereses y derechos en juego. Como es necesario esta ponderación de las circunstancias asociadas a cada pretensión de ejercicio individualmente considerada, teniendo presente el interés de los usuarios de tener acceso a esa información, se consideraran denegadas cuando se vea involucrada una figura, un referente, público, al igual que cuando por su naturaleza de interés público, no serán aceptadas, por producir un desequilibrio entre los derechos e intereses en juego.

4.5. LEGISLACIÓN Y PRECEPTO QUE RECOGE EL DERECHO AL OLVIDO.

Para regular el derecho al olvido, se instauró el Código del Derecho al Olvido[43], con el fin de divulgarlo, para hacer llegar a juristas y ciudadanos las normas que guían esta materia.

Este código busca solucionar las dudas que surjan sobre el ejercicio y disposición del derecho al olvido en lo referente a la aplicación de datos de carácter personal en el ámbito de internet. Además de almacenar y recopilar una amplia gama de normas distintas y las respectivas circunstancias en las que deben actuar, entre las que destacamos: rectificación de informaciones, sociedad de la información, respeto del derecho a la propia imagen, intimidad y al honor, protección de datos de registros (civil, penal, administrativos…).

El Código, recoge tanto leyes nacionales, como normativa europea que afecta a este derecho, con el fin de un conocimiento por los juristas y ciudadanos de su marco legal. Estableciendo este código una visión total de la legislación a la que repercute, para un mejor manejo de los ciudadanos de sus derechos. Hablamos de una diversidad de normas, puesto que, se mencionan, normas constitucionales, penales, civiles, sociales…

Son documentos primarios: libros, revistas científicas y de entretenimiento, periódicos, diarios, documentos oficiales de instituciones públicas, informes técnicos y de investigación de instituciones públicas o privadas, patentes, normas técnicas.

[43] Se encuentra recogido en el BOE.
http://boe.es/legislacion/codigos/codigo.php?id=094_codigo_del_derecho__al_olvido&modo=1

Para reforzar esta facilidad de acceso al código por cualquier interesado (ya sea un ciudadano o un profesional de la materia), el mismo se encuentra disponible para su descarga y visualización online. A partir de la aprobación del derecho al olvido en internet por la Justicia Europea, muchos son los que han acudido al ejercicio de este derecho.

Entendemos la importancia de la salvaguarda de los derechos relacionados con la privacidad e intimidad de los datos personales en una época en la que tenemos al alcance todo tipo de información con un solo "click", independientemente de su veracidad o aproximación a la realidad. Por ello asemejamos el derecho al olvido con el "derecho a vivir en paz"

4.6 SANCIONES POR INCUMPLIMIENTO DEL DERECHO AL OLVIDO.

Los miembros de la UE se reunieron en mayo de 2015 para revisar las obsoletas leyes que había respecto al tema, tratando de armonizar la regulación y conseguir un mejor uso de internet.

Se propuso un sistema de multa dividido en 3 niveles, multas para aquellas entidades que no respeten las reglas e incumplan las normas del derecho al olvido. Estas multas oscilarían entre el 0,5% y el 2% de los ingresos anuales de dichas compañías, atendiendo en cada caso a la gravedad de la infracción cometida.

Ante la conducta de no borrar la información personal, cuando proceda borrar esos datos, encaja en la segunda categoría, la cual asigna multas del 1% de los ingresos anuales de la entidad.

4.7. RESOLUCIONES AEPD.

Como mencionamos anteriormente, en ocasiones, tras las negativas de las entidades ante la pretensión de los sujetos interesados en el ejercicio del derecho al olvido o la insatisfacción de la respuestas de las entidades, estos acuden a la AEPD para que le ejerza la tutela de dicho derecho. Vamos a citar algunas de las resoluciones que esta agencia da a quienes acuden a ella:

- RESOLUCIÓN No.: R/02182/2016.

El reclamante ejercitó el derecho de cancelación de sus datos personales ante YAHOO INERIA SL, solicitando que sus datos no quedaran vinculados por YAHOO al realizar una búsqueda por su nombre. Alegando que *"A pesar de que el enlace ya no contiene mis datos, estos sí se ven en las cachés de Yahoo, tanto la interna como la externa."*.

YAHOO le respondió diciendo que no era el responsable del servicio de búsqueda, diciéndole que debe ejercitar su reclamación ante otra entidad. Ante tal comunicación, la cual no le pareció adecuada, solicito tutela por parte de la AEPD.

La AEPD resolvió lo siguiente: *"PRIMERO: DESESTIMAR la reclamación formulada por don B.B.B. contra la entidad YAHOO EMEA Ltd.*

SEGUNDO: NOTIFICAR la presente resolución a don B.B.B. y a la entidad YAHOO IBERIA, S.L., como establecimiento del responsable en España para que dé traslado de la misma a Yahoo Emea Ltd.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 18.4 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa (en lo sucesivo LJCA), en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal".

- RESOLUCIÓN No.: R/00308/2015.

Al no haberse atendido de manera adecuada el derecho a la cancelación pretendido por la representada de la reclamante frente a Google, se acudió a la tutela de esta agencia.

Analizados los documentos aportados con la citada reclamación, se observa que es necesario la subsanación. Solicitando para ello, con base en el art. 71 de la LRJPAC[44]:

[44] Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

- *"Acreditación del escrito de solicitud del ejercicio de derecho y la recepción del mismo ante el responsable del fichero.*
- *Impresión de las pantallas a las que se accede a través de los enlaces citados, resaltando los datos del afectado y la información que le afecta."*

Al recibir la agencia dicha información, se informa que según el 42.5 de la LRJPAC, que el plazo para notificar si se da o no la tutela queda suspendido por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario. A partir de la fecha de subsanación, computa el plazo para resolver el procedimiento.

El Director de la Agencia Española de Protección de Datos[45] resolvió: *"PRIMERO: INADMITIR la reclamación formulada por Da M.M.M. (Representada por D.*
N.N.N.) contra GOOGLE INC. (GOOGLE SPAIN).
SEGUNDO: INADMITIR la reclamación formulada por Da M.M.M. (Representada por
D. N.N.N.) contra D. O.O.O..).
TERCERO: NOTIFICAR la presente resolución a Da M.M.M. (Representada por D.
N.N.N.).
De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del RLOPD.
Contra esta resolución, que pone fin a la vía administrativa (artículo 18.4 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la LRJPAC, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso- Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal."

[45] José Luis Rodríguez Álvarez, Director de la Agencia Española de Protección de Datos.

5. CONCLUSIONES.

Podemos diferenciar dos ámbitos diferenciados que a su vez encuentran una estrecha vinculación entre ellos, por un lado nos encontramos con la sociedad, a nivel físico, tangible, donde los bienes jurídicos en juego sufren una afectación también física y tangible, y por otro lado encontramos el ámbito virtual, al que accedemos y el que vulneramos a trastes de las nuevas tecnologías, vulnerando esos mismos bienes jurídicos, actualizando los delitos tradicionales o bien a través de nuevas modalidades de delitos. Hay que puntualizar la lejanía del autor del delito en lugar del crimen en el caso de los delitos virtuales, ya que puede encontrarse incluso en la otra punta del mundo.

En los últimos años se ha ampliado el ámbito punible respecto a estos delitos cometidos mediante las nuevas tecnologías, a través de una imputación con forma desformalizada, que componen el estatuto jurídico-penal autónomo de la sociedad de la información[46], además del derecho penal tradicional.

Las nuevas tecnologías son un arma de doble filo, porque han supuesto innumerables mejoras en la sociedad, facilitando algunas labores, acercando a personas, o permitiendo el acceso a información necesaria para la realización de estudios, trabajos, investigaciones, etc… pero a su vez esto es algo que puede volverse contra las personas, ya que igual que facilita labores que son atípicas, facilita a los delincuentes la práctica de algunos delitos, y lo que más beneficia a estos es la dificultad que en ocasiones supone la localización de los mismos, y la extraterritorialidad y conflicto de leyes que puede suponer que el delito se cometa en un lugar diferente al del lugar del crimen.

En la actual política criminal, encontramos una característica común, esta es la intención de incorporar unos modelos de control universales, generales, e indiscriminatorios, suponiendo tal mediada un retraso por renunciar a resoluciones más avanzadas a nivel jurídico, que son más precisas, que respeten las exigencias de eficacia y garantía[47].

Ahora bien, respecto al derecho al olvido, decir que en nuestra sociedad, en la época actual, es un derecho necesario, ya que si no dispusiéramos de un derecho que permitiese cancelar nuestros datos y borrarlos del acceso de cualquiera, pondríamos en peligro nuestra intimidad, honor e integridad moral. El derecho al olvido en una sociedad tan informatizada es fundamental a la hora de reservar

[46] Crítico respecto de esta orientación, Hoyer, según la referencia de Jeßberger/Kreuß, como en la nota 34, p. 828.

[47] Enrique Anarte Borrallo "Crónicas Iberoamericanas. Informe sobre Criminalidad Organizada. España", RP 2, 1998, p. 103.

nuestra privacidad, permitiéndonos reservarnos esa información que no sea de interés publico ni este rodeada de relevancia para los demás.

Y es que como dijo el profesor Fernando Pérez Álvarez *"Uno de los retos que las Tecnologías de la Información y la Comunicación plantean es el referido a la seguridad. Los recursos que posibilita la tecnología para comunicar e informar, facilitan y satisfacen seguridad y libertades pero, a la par, comprometen expectativas y vulneran auténticos bienes jurídicos o derechos, que se conforman como valiosos para la convivencia social. La presencia de tales contextos define la (in) seguridad ante las Tecnologías de la Información y Comunicación".*

6. BIBLIOGRAFIA UTILIZADA

- AAVV, Las nuevas tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. mecanismos jurídicos de protección: carencias, interrogantes y retos del legisladoR Rev. Boliv. de Derecho No 23, enero 2017, ISSN: 2070-8157, pp. 168-191.

- ALLER, Germán, Cuestiones Victimológicas de Actualidad: Origen de la Victimología, Seguridad, Cifra Negra, Personalización del Conflito y Proceso Penal. ILANUD 27.

- ANARTE BORRALLO, Enrique, Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información. Universidad de Huelva. 2016.

- DOMÍNGUEZ MEJÍAS, Ignacio, Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española, Universidad de Sevilla, 2014.

- FERNANDEZ TERUELO, Javier Gustavo, Derecho penal e internet, especial consideración de los delitos que afectan a los jóvenes y adolescentes, lex nova, 2013.

- HERNANDEZ RAMOS, Mario, Derecho al olvido en Internet Cátedra de seguridad, Universidad de Salamanca , 2014.

- http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

- https://confilegal.com/20161109-las-nuevas-tecnologias-los-delitos-informaticos/

- NAVA GARCÉS, Alberto, Delitos informáticos, Editorial Porrua, 2016.

- POVEDA CRIADO, Miguel Ángel, Delitos en la red, cibercrimen ciberdelito, ciberespionaje y ciberterrorismo Ed. Fragua, 2011.

- TIRADO ESTRADA, Jesús José, la protección penal de la propiedad intelectual en la era digital (análisis tras la reforma del Código penal de 2015).

- VILLENA SALDAÑA, David, Derecho al olvido en Internet: Google y la doctrina europea. (Universidad Nacional Mayor de San Marcos, Perú).