FACULTAD DE COMUNICACIÓN

UNIVERSIDAD DE SEVILLA

GRADO EN PERIODISMO

TRABAJO DE FIN DE GRADO

Términos y condiciones de uso en Internet:

La Normativa es inútil sin la autorregulación del usuario.

Alumna: Blanca Delgado López

Tutor: Daniel Guerra Sesma

Términos y condiciones de uso en Internet: La Normativa es inútil sin la autorregulación del usuario.

Índice:

Términos y condiciones de uso en Internet: La Normativa es inútil sin la autorregulación del usuario.

1.- RESUMEN

El avance de las nuevas tecnologías, el big data o el uso de las redes sociales son algunas de las razones por las que el usuario cada vez, ofrece más datos personales a plataformas en línea, sin tener en cuenta la seguridad que podríamos estar vulnerando, ni las consecuencias que pueden surgir en un futuro. En la actualidad, crece el número de denuncias sobre el uso fraudulento de los datos que se han ofrecido de forma voluntaria en internet, o que un tercero ha publicado sin consentimiento. De esta forma, existen cada vez más publicaciones en línea que atentan contra derechos fundamentales de la persona como el derecho al honor, la intimidad o la propia imagen. Reluce así, la necesidad de una regulación sobre el uso de los datos en línea, pero encontramos que la legislación actual se encuentra obsoleta en comparación con la rapidez con la que avanza el uso de las nuevas tecnologías. Por ello, cobra más importancia la autorregulación y cautela del usuario frente a la publicación de ciertos datos.

2.- PALABRAS CLAVE

Derecho - Internet - Big Data - Autorregulación - Contenido - Digital - Seguridad - Redes Sociales - Datos Personales

3.- INTRODUCCIÓN

Periodismo tradicional y periodismo digital, son conceptos que nos dicen la evolución que ha sufrido la forma de comunicarnos. Hoy día no podemos pensar en el mundo sin internet y todos los usos derivados de la red. Pero no podemos analizar las oportunidades que ofrece el uso de las nuevas tecnologías, sin tener en cuenta el importante riesgo que supone para los ciudadanos el mal uso de estas.

El objetivo principal de este trabajo se centrará en aportar una mayor información a los usuarios de la red para facilitar y ayudar a la toma de decisiones. La información de cómo funciona la red, donde van a parar nuestros datos personales, que uso hacen de ellos y en definitiva que consecuencias se pueden derivar de la subida indiscriminada a de datos a la red, debe ser la aportación que justifica este estudio y el interés de nuestra investigación. Nuestro interés es dar una mayor claridad y ordenar las ideas en el uso de esta intrincada red que es la world wide web.

La sociedad demanda una mayor regulación por parte de las administraciones que proteja los intereses de los usuarios que utilizamos internet, y hacemos uso de todas sus variantes: la propia red, navegadores, motores de búsqueda, apps, redes sociales, etc. , demandamos que nos defiendan, pero ¿somos conscientes de que nosotros mismos como usuarios somos los que ponemos nuestra seguridad en peligro?, ¿somos conscientes de que los datos con los que dañan nuestra propia imagen y atentan contra nuestros derechos al honor y la intimidad los hemos facilitado nosotros mismos, o en cualquier caso, hemos autorizado a otros su difusión?

Comenzaremos dando una visión del panorama actual para pasar al análisis del marco legislativo vigente, tanto a nivel europeo como nacional, así como las instituciones más importantes que intervienen en la regulación del mismo.

A continuación, y vinculado y derivado del marco legislativo, analizaremos algunos aspectos de la privacidad y datos públicos en internet, haciendo referencia al concepto de Big Data, y a las publicaciones en Internet, datos que se facilitan y leyes que lo regulan. Asimismo, explicaremos el tan conocido ya como “Derecho al Olvido”, la libertad de Información y la libertad de Expresión, el Derecho al Honor, Intimidad y Propia Imagen.

No podemos terminar este análisis sin dedicarle un capítulo especial a las Redes Sociales más comúnmente usadas: Facebook, Instagram y Twitter.

La metodología inicial que hemos utilizado para realizar nuestro trabajo ha sido la Investigación Hemerográfica, que, en palabras de Vanessa Rangel Maldonado, consiste en la búsqueda de conceptos, teorías, criterios, en libros, revistas, periódicos y otro tipo de material impreso, o en nuestro caso, en páginas web.

La metodología práctica ha consistido en realizar una serie de preguntas de forma on-line utilizando la herramienta metodológica del análisis cuantitativo, que es aquel que busca establecer la cantidad de algún elemento presente en una muestra.
Utilizamos esta metodología porque consideramos que es la más adecuada a los objetivos de información para el análisis del comportamiento y evolución por tramos de edades, que pretendemos conseguir.

Y por último estableceremos unas conclusiones y tendencias hacia las que entendemos que se dirige el mundo de la red.

4.- HIPÓTESIS Y OBJETIVOS

4.1 - HIPÓTESIS

La hipótesis inicial con la que comenzamos esta investigación es demostrar la cantidad de datos personales que ofrecemos en distintas redes sociales y plataformas online de forma indiscriminada, sin tener en cuenta la repercusión que puede conllevar. Además del desconocimiento de la legislación vigente que regula todo el contenido digital.

4.2. - OBJETIVOS

El principal objetivo de "*Términos y condiciones de uso en Internet: La Normativa es inútil sin la autorregulación del usuario."* es CONCIENCIAR sobre la importancia de la autorregulación y prudencia del usuario frente a la publicación de contenido o aportación de datos personales en internet, así como la educación en un uso responsable de las principales plataformas en línea y redes sociales.

- Identificar un uso seguro de la publicación de contenidos digitales y datos personales en línea.
- Aprender a utilizar las nuevas tecnologías de una forma prudente obteniendo el máximo rendimiento de sus aplicaciones y programas.
- Reflexionar sobre los datos o contenidos que debemos o no publicar en internet, conociendo su posible repercusión futura.
- Conocer los derechos que se pueden reclamar y delitos que pueden realizarse de forma inocente.
- Determinar si existe o no la necesidad de actualizar la legislación vigente.

5. MARCO TEÓRICO

5.1- PANORAMA ACTUAL

Internet ha revolucionado la forma en la que nos comunicamos de una forma radical. Actualmente, es muy complicado concebir la vida diaria, el ocio o el ámbito laboral sin internet. De hecho, la necesidad constante de conexión wifi por parte de muchas personas de la sociedad se considera incluso una enfermedad diagnosticada. Hoy en día, disponemos de terminales móviles inteligentes con una tecnología, por la que enviamos y recibimos información a todo el mundo de forma instantánea. Estos terminales son capaces incluso, de conectarse con otros dispositivos cotidianos como un vehículo o la domótica de un hogar. Lo que se conoce como “el internet de las cosas”. Según Hans Vestberg, CEO de Ericsson: "Si una persona se conecta a la red, le cambia la vida. Pero si todos los objetos de su vida se conectan, el mundo cambia". Actualmente nos encontramos inmersos en este cambio. Un fenómeno social que junto a una tecnología favorecedora que cambia día a día, hace que cambie nuestra forma de relacionarnos.

La velocidad, el acceso a multitud de recursos, la documentación, la agilidad en el ámbito laboral, la interconexión a nivel mundial, y la recepción de información al segundo, son algunas de las ventajas de este nuevo paradigma de la comunicación digital que encontramos en nuestra sociedad actual. Según el estudio del Institute Advertising Bureau (IAB) sobre los medios de comunicación digital, el 96 % de la población española navega en Internet entre 6 o 7 días a la semana. La mayor frecuencia de conexión la tienen los buscadores con un uso diario del 80 % de los internautas, seguido por las redes sociales y los medios de comunicación digital. Llama la atención que el uso del Smartphone y la Tablet crece de forma exponencial alcanzando el uso del ordenador para el acceso a esta información.

La audiencia cada vez está más informada, reclama más datos y son capaces de conseguirlo todo a través de su propio teléfono móvil. El proceso de la digitalización se ha quedado obsoleto y ahora las tecnologías de inteligencia e innovación van mucho más allá. El uso de dispositivos inteligentes es cada vez más frecuente entre la población, y los hábitos del consumidor cambian al mismo tiempo.

El uso de aplicaciones en estos dispositivos en la mayoría de las ocasiones, conlleva el registro del usuario con algunos datos personales, descarga de aplicaciones adicionales, o pagos a través de la tarjeta de crédito. Además, cada vez son más los dispositivos que se conectan con nuestro teléfono móvil, y éste es la herramienta más valiosa de la que dispone cada persona. Ya que con él se tiene un acceso directo a prácticamente toda nuestra vida diaria, laboral y a nuestros datos personales. Millones de datos personales colgados en los servidores de Internet, a veces con consentimiento del usuario, y a veces ofrecidos por terceros, que, sin precaución alguna, son subidos a la red sin conocerse a ciencia cierta la repercusión que puede tener.

Además, también existe una necesidad social de interactuar en Internet, subir fotografías, aportar opiniones, gustos y aspectos sensibles de la vida de cada persona. Datos que, en la vida offline, no comunicaríamos con tanta facilidad, incluso preservaríamos con mucha cautela, y más tratándose de ofrecer estos datos a un desconocido. Partiendo de la premisa de que toda nuestra vida está en línea y se pueden hacer informes exhaustivos de nuestro día a día y nuestra personalidad, únicamente indagando en la red. La información es poder, y todos estos datos son prácticamente públicos, y la facilidad de su difusión, incluso, comercialización es casi infinita.

La legislación determina una serie de sanciones si alguno de estos casos se produce sin nuestro consentimiento, si nuestros datos se utilizan de forma fraudulenta o si se difunde algún dato que pueda perjudicarnos. Pero hoy en día, nos encontramos situaciones como el acceso a nuestro correo electrónico, algo que, si se utiliza con frecuencia en el ámbito personal o laboral, puede poner a libre disposición mucha información sensible de una persona. El secreto de las comunicaciones, un derecho constitucional nacional, actuaría en el caso de que se difundiese información considerando que se obtiene de forma ilícita. Pero ¿qué ocurre si perdemos algún dispositivo en el que no se tenga guardada la contraseña, dejamos la sesión abierta en algún ordenador que no es nuestro o alguien entra en él con nuestra clave? Aunque el delito está claro y su resolución debe darse en los juzgados, será muy complejo eliminar por completo la información que se ha podido difundir en Internet, y que pueda perjudicarnos, y el proceso judicial en el que nos veremos inmersos será muy complicado.

Del mismo modo, en muchas ocasiones un tercero puede difundir información en redes sociales que atenta contra derechos de honor, intimidad o propia imagen de una persona. Si esta información se difunde sin nuestro consentimiento, o simplemente es utilizada en nuestro

perjuicio, daría lugar a un conflicto judicial, que curiosamente cada vez surgen con más frecuencia en la sociedad.

Lo mismo ocurre si consideramos el negocio que supone la compra venta de bases de datos entre empresas. Puede parecer algo descabellado, pero al final son datos que propiciamos de forma inconsciente al aceptar que se comercialice con nuestros datos, cuando confirmamos los aspectos y condiciones de uso, o al exhibir de forma pública en internet aspectos privados de la vida personal o laboral. La legislación actual protege estos datos, y su uso siempre debe estar autorizado por el usuario. Pero son muy pocos los que leen los términos y condiciones de uso de los datos personales al registrarse en una web o crear perfiles en alguna red social.

Por ello en muchas ocasiones, no se debe culpar únicamente al que difunde, vende o filtra una información, dado que la cesión de datos personales a terceros en multitud de ocasiones es un problema de uno mismo, que no ha sido consecuente o que ha firmado un consentimiento, siendo inconsciente de su repercusión, aceptando los términos y condiciones de uso de alguna red social o web.

En un ámbito laboral, internet y las redes sociales han supuesto otro cambio fundamental en la sociedad actual. No solo por lo que supone el uso del correo electrónico, que todo un archivo de documentación esté digitalizado, o las nuevas estrategias de marketing y promoción de productos que ha facilitado el ámbito online. Internet se posiciona como una herramienta necesaria en la mayoría de los negocios actuales. Ahora bien, ¿es lícito que una empresa investigue un correo electrónico profesional, o el historial de navegación de un trabajador?

Se puede considerar una intromisión en la intimidad del trabajador, pero si la empresa deja constancia por escrito del uso de Internet durante el horario laboral, y el trabajador lo asume, no podría existir ninguna queja al respecto. Lo mismo sucede con las redes sociales. Las redes sociales son una herramienta para conseguir visibilidad, promoción y acciones de marketing para empresas que implantan una filosofía 2.0. El uso de redes sociales como Facebook o Twitter, en algunos puestos de trabajo se considera una pérdida de tiempo en el trabajo, y en otras es una parte fundamental de la actividad de la empresa. Recientemente hablamos de nuevos perfiles y nuevos trabajos que surgen de este nuevo paradigma digital. Como son los Millennials.

Desde hace algunos años estamos viendo como los medios de comunicación actuales hacen alusión a un sector muy amplio de la sociedad joven, a los que le denominan los "Millennials". Son todas aquellas generaciones nacidas a finales del siglo XX, que se encuentran totalmente influidos por el ámbito digital y el cambio del milenio. Es decir, todos aquellos que en cierta forma conocen cómo era el mundo sin internet, pero que han crecido de la mano de las nuevas tecnologías, por lo que actualmente son los que conectan a las generaciones longevas con este nuevo paradigma. Un modelo que hace tener una dependencia absoluta a la tecnología, ya que se obtiene a golpe de click todo lo que uno desea, que se vive de la mano de la información y podríamos decir que, en la mayoría de los casos, la sociedad del primer mundo sufre un fenómeno de "Infoxicación" o trastorno producido por el exceso de información.

Nos encontramos pues con una generación, con alto nivel cultural, destreza digital, caracterizados por el emprendimiento. Curiosos e inconformistas que no solo buscan y se nutren de la información diaria de los medios de comunicación e Internet, sino que son característicos porque participan de ella. Comparten, opinan, debaten e interactúan a nivel global gracias a las nuevas tecnologías. Creando de esta forma un nuevo paradigma de la comunicación que se basa en un modelo circular, en el que cobra más importancia el feedback de la comunicación, que el propio mensaje inicial que quiera transmitirse. Una revolución que deriva en la sobrecarga de información en muchos casos gracias a la facilidad del uso de plataformas que fomentan el conocimiento colectivo de cualquier tema, dado que todo está en internet.

Nick Jones, vicepresidente ejecutivo de innovación y crecimiento en Arc World wide, hizo unas declaraciones al respecto de todo ello en uno de los principales congresos a nivel mundial sobre innovación y tecnología, que se celebra en Barcelona (Mobile World wide Congress 2016): *"La nueva generación de Millennials e incluso los públicos más jóvenes están cada vez más familiarizados con este tipo de mundo. Donde no hay tanta protección de la privacidad (...) Ven esto como un valor, más que una intromisión en su intimidad"*

Afirmó que las generaciones de los jóvenes están cada vez más dispuestas a recibir información y publicidad de las marcas, a través de las nuevas tecnologías, siempre y cuando sientan que son contenidos personalizados. Para conseguir esto es imprescindible conocer cada vez más y más datos personales, o el estilo de vida de cada individuo. Algo que roza los

límites de la privacidad y la intimidad de las personas, y para conseguirlo es necesario el intrusismo en el uso de Internet, así como en el de los dispositivos electrónicos de uso diario.

Un líder o modelo de esta generación es Mark Zuckerberg. Un joven Millennial que ha cambiado por completo el modelo de la comunicación al crear la red social Facebook. Jugando entre las esferas más personales que existen en la vida de cualquier individuo, su biografía y sus contactos. Un juego, al que se han visto obligadas a participar las empresas, ya que en esta red social se encuentra prácticamente toda la información que necesitan sobre sus clientes potenciales, obtienen visibilidad mundial, y reciben un feedback casi instantáneo de su relación con el cliente.

CASO MARK ZUCKERBERG Y CAMBRIDGE ANALYTICA.

El pasado 24 de mayo Mark Zuckerberg se enfrentó a la Euro Cámara para pedir disculpas sobre la actuación de la red social tras el escándalo de Cambridge Analytics. Zuckerberg afirmó que la red social que cuenta con millones de usuarios en todo el mundo, *"no hizo lo suficiente para evitar que distintas herramientas de Facebook se utilizasen para hacer daño".* Para ello, propone acatar el nuevo Reglamento Europeo de Protección de Datos en sus políticas de privacidad, así como aumentar la seguridad y la gestión de los datos de los usuarios. Aunque actualmente persisten las políticas de la compañía que permiten el traspaso de ciertos datos a terceros.

El escándalo de Cambridge Analytics se basó en el robo de información de millones de usuarios, a través de aplicaciones que se conectaban con el perfil de Facebook, accedían a la información y además permitían el acceso a la información de los amigos de este perfil, lo que multiplicaba exponencialmente el número de datos. Actualmente se investiga la implicación que ha podido tener el uso de estos datos para crear anuncios personalizados para los usuarios en la campaña de las Elecciones de EEUU favoreciendo al actual presidente Donald Trump o en el Brexit en Inglaterra.

Sandy Parakilas, uno de los directivos responsables del traspaso de datos entre Facebook y otras empresas entre 2011 y 2012, asegura que *"La cantidad de datos que Facebook pasó a terceras empresas entre 2010 y 2014 fue ingente."* Decenas de miles de aplicaciones, probablemente cientos de miles, tenían acceso a los datos a través de la función de *"permiso*

para amigos". Este antiguo trabajador de la compañía relata que Facebook era consciente de lo que estaba sucediendo, pero que no se hizo nada al respecto hasta 2014. Por lo que, durante años, muchas empresas tuvieron la puerta abierta a esta obtención de datos, sin consentimiento alguno por parte de los usuarios.

"Cuando los datos pasaban del servidor de Facebook a los del desarrollador, la red social perdía el control por completo de esos datos. El gran problema es que Facebook permitía a estos desarrolladores acceder a datos privados de la gente sin su permiso expreso", ha detallado Parakilas. El primer gran fallo era permitir que eso ocurriera durante años. El segundo, no evitarlo ni hacer inspecciones a los desarrolladores que pudieran estar abusando de esos datos.

Giovanni Buttareli, Supervisor Europeo de Protección de Datos, afirma que: *"No fue por casualidad, no fue una fuga de datos, no fue un incumplimiento del contrato, sino el resultado de una práctica habitual y de un modelo de negocio dominante en la actualidad".*

El 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, conocido como Reglamento General de Protección de Datos de la Unión Europea, vigente a partir del 25 de mayo de 2018 exige que debe existir un consentimiento explícito del usuario sobre el uso de cualquier información personal por parte de la compañía. En el caso de Facebook el usuario deberá permitir o no el acceso a sus datos generados dentro y fuera de la red social, como las búsquedas en internet que se relacionen con un perfil. En caso contrario se prevén multas de hasta el 4 % de los ingresos globales de las empresas por violaciones de la privacidad.

Por lo que Facebook debe preguntar a los usuarios si prefieren optar o no a que sus datos se compartan con los anunciantes, para mejorar la experiencia del uso de la red social, si aceptas, pero no quieres que se acceda a tus datos personales serás un perfil "menos relevante" para Facebook y si no aceptas los términos y condiciones de uso de la red social, probablemente eliminen tu cuenta en unos 90 días.
Asimismo, este comportamiento por parte del usuario incide en el precio de la publicidad, ya que para el anunciante un perfil restringido no será tan interesante y reducirá el precio ofrecido.

5.2 - MARCO LEGISLATIVO

La Unión Europea hace balance sobre la importancia y las oportunidades que ofrece el uso de las nuevas tecnologías en la vida diaria de los ciudadanos, aunque también advierte sobre el riesgo que su mal uso puede ocasionar. Uno de los principales problemas que ofrece crear una normativa común europea es el carácter global que ofrece internet. Un ejemplo de esto son los servidores que almacenan toda la información y datos a los que accedemos cuando navegamos en la red. Estos servidores están situados en países distintos, por lo que la regulación también es distinta y las consecuencias de determinadas acciones o delitos también son diferentes. Esto genera incertidumbre sobre los tribunales competentes o la normativa que debe aplicarse.

El contexto global en Internet es complicado al contar con una pluralidad de estados. Es necesaria la adaptación del bloque normativo tanto europeo como nacional, a la realidad que nos inunda. Demandamos la necesidad de actualización de una legislación obsoleta. Asimismo, hay que especificar competencias de cada uno de los estados y regular responsabilidades, y establecer Protocolos de actuación con determinados casos ilícitos que se están produciendo con demasiada frecuencia.

Todo este panorama desemboca en que con la legislación existente no hay estabilidad jurídica. Hay que hacer una adaptación y reinterpretación de la legislación vigente. Se pone de manifiesto la necesidad de contar con un mínimo común normativo a todos los estados miembros de la UE.

Pero volvemos aquí a poner de manifiesto la dicotomía que planteábamos al comienzo del trabajo: Demandamos una regulación publica sin ser conscientes de que la autorregulación privada es tan necesaria como la anterior.

5.2.1- Europeo

El 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, conocido como Reglamento General de Protección de Datos de la Unión Europea, vigente a partir del 25 de mayo de 2018, es el marco legislativo europeo de referencia con el que contamos los países de la Unión.

El RGPD es una norma directamente aplicable, que no requiere normas internas de trasposición.

Una de las principales novedades que introduce este Reglamento, de acuerdo con la *"Guía del Reglamento General de Protección de datos para responsables de tratamiento"* está en el principio de responsabilidad proactiva, es decir, los responsables del tratamiento de datos tienen que aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento que se realiza de los datos es conforme al Reglamento. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones.

Asimismo, el Reglamento trata de manera muy especial las bases de legitimación para el tratamiento de datos, es decir, todo tratamiento de datos debe apoyarse en una base que lo legitime, fundamentalmente el Consentimiento. Éste debe ser inequívoco, es decir debe ser una manifestación del interesado mediante una clara acción afirmativa. A diferencia con el Reglamento de desarrollo de la LOPD, no se admiten formas de consentimiento tácitas o por omisión. Y si los datos son sensibles, el consentimiento debe ser además explícito. Incide también el Reglamento en que la información que se facilite a los interesados debe ser concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo.

Por otra parte, la Comisión Europea, en Bruselas mayo de 2015, emitió el documento: Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones, "Una Estrategia para el mercado único digital en Europa", en la que Jean Claude Juncker, su Presidente, comienza diciendo que:

"Creo que debemos utilizar mucho mejor las grandes oportunidades que ofrecen las tecnologías digitales, que no conocen fronteras. Para ello, necesitamos tener el valor de abrir los compartimentos nacionales de regulación de las telecomunicaciones, de derechos de propiedad intelectual y de legislación sobre protección de datos, de gestión de las ondas de radio y de aplicación del Derecho de la competencia."

El Tribunal de Justicia de Unión Europea, creado en 1.952, con sede en Luxemburgo, garantiza que la legislación europea se interprete y aplique de la misma manera en cada uno de los países miembros, y resuelve los litigios entre los gobiernos nacionales y las instituciones europeas.

Por otra parte, la Agencia Ciberseguridad de la UE, ENISA (European Union Agency for Network and Information Security), es la encargada de frenar los ataques y delitos informáticos, cada vez más frecuentes.

Entre otros organismos europeos que velan por la seguridad, incluidos los posibles delitos informáticos, debemos hacer referencia obligada a Europol, la agencia de la Unión Europea en materia policial, cuyo principal objetivo es contribuir a la consecución de una Europa más segura para beneficio de todos los ciudadanos de la UE, y Eurojust, órgano de la Unión Europea (UE) encargado del refuerzo de la cooperación judicial entre los Estados miembros, mediante la adopción de medidas estructurales que faciliten la mejor coordinación de las investigaciones y las actuaciones judiciales que cubren el territorio de más de un Estado miembro.

5.2.2. Nacional.

RD-Ley para adaptar el Derecho nacional al Reglamento Europeo de Protección de Datos.

El Gobierno español ha aprobado recientemente el Real Decreto-Ley 5/2018 de 27 de julio, de medidas urgentes para la adaptación del derecho español a la normativa de la Unión Europea, en materia de protección de datos, entra en vigor el 31 de julio, y regula cuestiones como la actividad de investigación plazos de prescripción y régimen sancionador, entre otras. La normativa a la que se adapta el derecho español es en concreto el 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 sus datos personales y a la libre circulación de estos datos, que es plenamente aplicable en España desde el pasado 25 de mayo.

Tal como explica la exposición de motivos del nuevo RD-Ley, la necesidad de adaptar el marco normativo interno al Reglamento General de Protección de Datos supuso asimismo la aprobación por el Consejo de Ministros en su sesión de 10 de noviembre de 2017 de un proyecto de ley orgánica, remitido a las Cortes Generales, que actualmente se encuentra en tramitación parlamentaria.

La Carta Magna española, la Constitución de 1978 establece en su Título I, de los derechos y deberes fundamentales, Capítulo segundo, Derechos y libertades, Sección 1.ª De los derechos fundamentales y de las libertades públicas:

Artículo 18:

1. **Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.**
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La Constitución, por tanto, es el principal texto legal en el que se ven reconocidos derechos que afectan directamente a cuestiones que pueden ponerse en peligro con el mal uso de internet: el honor, la intimidad personal y familiar y la propia imagen, derechos que tienen el rango de fundamentales.

Y hasta tal punto aparecen realzados en el texto constitucional estos derechos fundamentales, que el artículo 20.4.- dispone que el respeto a tales derechos constituye un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales:

Artículo 20.1. - Se reconocen y protegen los derechos:

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

b) A la producción y creación literaria, artística, científica y técnica.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

Artículo 20.4. - Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

Como desarrollo de estos puntos de la Constitución, se aprobó la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El 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, conocido como Reglamento General de Protección de Datos de la Unión Europea, vigente a partir del 25 de mayo de 2018, es el marco legislativo europeo de referencia con el que contamos los países de la Unión.
Como hemos dicho anteriormente, el RGPD es una norma directamente aplicable, que no requiere normas internas de trasposición.

Hasta el 25 de mayo de 2018, fecha de entrada en vigor del Reglamento UE 2016/679, en España todo estaba regulado por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPDCP), y su Reglamento de desarrollo (RLOPD) aprobado por el Real Decreto 1720/2007 de 21 de diciembre. Desde entonces, tanto el desarrollo tecnológico, como el acceso a la información, como el Big Data, ha crecido de forma exponencial. Y, además, al hablar de internet, estamos en un contexto global, sin fronteras. El nuevo Reglamento Europeo de Protección de Datos, especifica un marco jurídico mucho más estricto en cuanto a la accesibilidad de los datos personales que existen en internet.

Esta nueva regulación, que por primera vez se hace a través de un Reglamento Europeo, según resume la AVS de Gestores Públicos, implica cambios significativos en la protección de datos de carácter personal, tanto desde el punto de vista de los derechos de las personas, como de las obligaciones de las personas y entidades que tratan estos datos.

A partir del 25 de mayo de 2018 algunos aspectos de la LOPDCP y del RLOPD quedarán desplazados por el nuevo Reglamento Europeo, sin embargo, otros aspectos pueden seguir siendo aplicables, bien porque queden fuera del ámbito de aplicación del nuevo Reglamento o bien porque éste permita su regulación específica a los distintos estados.

De hecho, actualmente el Estado Español a través del Congreso de los Diputados, tiene en marcha un Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que fue publicado por el Boletín Oficial de las Cortes Generales el pasado 24 de noviembre de 2017.

Existen tres leyes que validarían el contrato entre un usuario y una empresa que guarda y almacena sus datos:

- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPDCP),
- La Ley 7/1998 de 13 de abril, sobre Condiciones Generales de la Contratación y
- La Ley 26/1984 de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

Si nos basamos en lo que determina la LOPDCP, para la obtención de este consentimiento, es fundamental y necesario que el usuario haya sido informado, para que sea un consentimiento válido: "Toda manifestación de voluntad, libre, específica e informada, mediante la cual el afectado consienta el tratamiento de los datos personales que le conciernen". Por ello, cuando, por ejemplo, se hace una actualización de los términos y condiciones de uso de una red social o un buscador, la plataforma impide continuar con su uso hasta que se acepta que se han leído y aceptado estos nuevos términos. Lo que supone un consentimiento expreso.

La LOPDCP, permite al responsable del fichero (con información) utilizar los datos de un usuario, si éste da su consentimiento expreso (Artículo 6.1), y en especial en el Artículo 11, regula la cesión de estos datos a un tercero. Si ahondamos en este artículo, mientras los datos pertenezcan a datos personales imprescindibles de un contrato, como todos los que sean necesarios, por ejemplo, para una compra, no sería necesario el consentimiento expreso del usuario, para el uso de la empresa en su beneficio de estos datos.

Tampoco sería necesario este consentimiento para ceder los datos a un tercero, en el caso de existir una aceptación que implique la necesidad de transmitir estos datos, como parte fundamental del cumplimiento del contrato. Es decir, por ejemplo, si una agencia de viajes debe dar los datos a una aerolínea para contratar unos vuelos que ha pedido expresamente un usuario. Y, por último, tampoco sería necesario el consentimiento del usuario y la cesión de

estos datos a un tercero, siempre y cuando los datos obtenidos han sido recabados de fuentes accesibles al público. Creando así bases de datos para estrategias comerciales o publicitarias, que nunca deben atentar contra los derechos fundamentales del usuario y debe permitirles de una forma fácil y gratuita, darse de baja de estos ficheros.

Se consideran fuentes accesibles al público los Boletines Oficiales del Estado o los medios de comunicación. Ahora bien, en el caso de no haber fijado unos criterios de privacidad específicos en las redes sociales, toda la información que se encuentre en ellas que tengan un carácter público, es información pública que ha facilitado el propio usuario. También es necesario considerar que la LOPDCP en su artículo 15 considera el derecho al usuario de solicitar y obtener gratuitamente información de sus datos, el uso que se les da y el origen de la obtención de los mismos.

Algo que también recaba información sobre nuestro uso de Internet y que es utilizado por las empresas son las cookies. Son un software que se descarga automáticamente en nuestro ordenador desde distintas páginas web, que registran nuestra forma de interactuar con ellas. Los productos que vemos en una tienda online, los lugares que a los que nos gustaría viajar, o información que obtengamos de los buscadores. Normalmente funcionan en beneficio del usuario, para mejorar su experiencia online, que recuerde datos y contraseñas para facilitar la navegación y en otras ocasiones funcionan en beneficio de terceros que, utilizan esta información para hacer estudios sobre el comportamiento del usuario.

El apartado segundo del Artículo 22 de la Ley 34/2002 de 11 de julio (LSSI) de Servicios de la Sociedad de la Información y del Comercio Electrónico, establece que se debe facilitar a los usuarios información clara y completa sobre el uso de las cookies. Por ello existe una regulación comunitaria y nacional que obliga a informar a los usuarios sobre el uso de las cookies. Además, debe existir un consentimiento claro por parte de la persona que navegue en una web, de que conoce las políticas de cookies y protección de datos del sitio web en el que navegan. Con más importancia en aquellas páginas web en las que se aporte información personal. Como, por ejemplo, la web de una entidad bancaria, en la que su política de privacidad y protección de datos es mucho más estricta. Lo que no exceptúa, que una entidad bancaria pueda conocer lo que compras, cómo lo compras y cuándo sueles comprar, con vista a ofrecerte productos financieros a tu medida, además de comprobar si serías un cliente fiable para un crédito.

El uso de las cookies ha quedado regulado actualmente con la denominada Ley de Cookies, Real Decreto - Ley 13/2012 de 30 de marzo, que obliga a la información del uso de los datos que recabe este software instalado en nuestro ordenador, así como la necesidad de autorización del usuario para la descarga de las mismas. Existen páginas web que no dejan navegar en ellas, si no se autoriza expresamente la descarga y uso de la información de sus cookies. Ya que las páginas web que utilicen los datos de las cookies están obligadas a disponer del consentimiento del usuario.

Renovando la jurisdicción obsoleta que encontramos, en un panorama novedoso, en el que todavía existen algunos vacíos legales, en cuanto a procesos jurídicos a seguir, en caso de que se vulneren derechos fundamentales. Como el Derecho al Honor, Intimidad o Propia Imagen, incluso al secreto de las comunicaciones. De esta forma, este nuevo Reglamento incluye sanciones, obligación de informar al usuario europeo y nuevos derechos como el derecho al olvido.

Por último, no podemos cerrar este capítulo dedicado a la normativa sin hacer referencia la derecho de propiedad intelectual, recogida en el artículo 27.2 de la Declaración Universal de los Derechos Humanos, y regulada en España mediante el 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 en la materia. En España, en la propiedad intelectual se integran los derechos de autor y los derechos vecinos afines.

Es evidente que Internet ha supuesto un impacto tremendo sobre los derechos de autor, ya que, como dice Alejandro Puerto Mendoza en su obra “Introducción al derecho de Internet”, Madrid 2015, con la aparición de esa red informática mundial se ha producido un cambio radical en la forma de crear y distribuir contenidos, lo que ha provocado la quiebra del sistema vigente: son nuevos desafíos para el derecho y la necesidad de instaurar un nuevo escenario que satisfaga a todos los actores. Los modelos de protección de los derechos de autor que se han venido ejerciendo tradicionalmente ya no sirven en Internet.

5.3 Aspectos de Privacidad y datos públicos en internet.

3.1. Big Data.

Los responsables de empresas y negocios llevan años utilizando distintas estrategias para captar clientes, obtener una buena base de datos y analizarla para elaborar un cliente, tipo que les ayude a tomar decisiones y obtener beneficios. La tecnología actual hace que se cuente con mecanismos rápidos e innovadores que permiten crear perfiles generales y específicos de una persona desde un ordenador.

Cada vez que navegamos en internet, hacemos una búsqueda, interactuamos en una red social, vemos las características de un producto en Amazon o nos hacemos amigos de algún contacto en Facebook, se queda registrado en lo que llamamos Big Data. Es un término que alude al almacenamiento, clasificación y análisis de todos los datos que existen en línea de cada persona, y que al mismo tiempo se relacionan entre ellos para mejorar la experiencia del usuario. Entre los nuevos perfiles más demandados a nivel internacional por el ámbito laboral, son aquellos se sean capaces de recopilar, analizar y obtener información de los clientes potenciales de una empresa, a través del Big Data. Integrar todos los datos y plantear mejoras, tomar decisiones y nuevas conclusiones para la obtención de beneficios de la marca.

Las empresas centradas en la obtención y análisis de estos datos son una de las más poderosas del planeta, casi en el mismo eslabón que las empresas petrolíferas. Ejemplos de ello, es el poder de Google o de la red social Facebook. Toda nuestra información se encuentra almacenada en distintos servidores que funcionan a nivel internacional. Algo que dificulta un proceso judicial ya que la empresa que utiliza unos datos, está en un país, pero el servidor que los almacena está en otro, y la legislación aplicable puede ser totalmente distinta. Esto es lo que sucede con los problemas relacionados con la propiedad intelectual, o la protección de datos.

El nuevo entorno digital, encuentra su clave en establecer que todos los servicios que ofrece sean gratuitos, en facilitar la información de los usuarios a terceros. Ahora bien, para realizar estas prácticas el empresario debe disponer del consentimiento del usuario para este proceso, además de garantizar que se le ha informado debidamente de ello.

Internet ha facilitado la clasificación y el tratamiento de la ingente cantidad de datos que almacenan estos servidores, creando cruces de datos, informaciones y análisis relacionados con cada uno de los usuarios, y con la forma en la que interactúan con internet.

Para beneficiarse de estos datos o esta información, las empresas deben justificar el consentimiento del usuario. Algo que vemos de forma habitual cuando para crear un perfil, un correo electrónico, o realizar una compra, es necesario *"aceptar los términos y condiciones de uso"*. Si no se aceptan, la plataforma online impide avanzar en el proceso. Esta aceptación se considera un consentimiento, o lo que es lo mismo en el ámbito offline, la firma de un contrato.

5.3.2.- Publicaciones en Internet, datos que se facilitan y leyes que lo regulan.

Según la Agencia Española de Protección de Datos, entre los datos voluntarios que ofrecen las personas cada vez que se registran en una web, hacen una compra, o crean una cuenta en redes sociales, encontramos el nombre, el apellido, el correo electrónico, el teléfono de contacto, fecha de nacimiento, domicilio y país de residencia. Con algunas compras, es necesaria la identificación del DNI y los dígitos de la tarjeta de crédito. Por tanto, con un uso simple de internet se detallan suficientes datos para identificar, localizar, conocer hábitos de conducta o estilo de vida de una persona. Lo que puede afectar a la seguridad.

También es necesario incluir los datos que son publicados en internet por terceros. Debido a que una persona puede ser muy consciente, y cuidadoso, con la información que publica de uno mismo en internet, pero en el momento que un conocido alude a una persona en sus redes sociales, blog, descripciones de vídeos o foros, ya se encuentran fotografías e información sobre una persona con una búsqueda.

Además de directorios online o medios de comunicación en los que se identifique a una persona, en publicaciones académicas, o si por algún motivo el nombre de una persona aparece en el Boletín Oficial del Estado, o en alguna resolución de la Administración Pública, se revelan datos personales de acceso público que son capaces de indexar o rastrear los buscadores.

RIESGOS SEGÚN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Las páginas web de la Agencia Española de Protección de Datos, https://www.aepd.es/, y del INCIBE https://www.incibe.es/ tienen una gran cantidad de información que todos debíamos conocer para hacer un buen uso de Internet.

Entre sus publicaciones tiene una Guía sobre "Privacidad y seguridad en Internet", realizada en colaboración con el Instituto Nacional de Ciberseguridad, INCIBE y la Oficina de Seguridad del Internauta, en la que en 18 Fichas hacen un repaso sobre los principales peligros a los que nos vemos expuestos en el uso diario de nuestro ordenador, smartphone, o tablet, entre los que podemos destacar:

- Cuando compramos a través de Internet, uno de los riesgos más habituales es ofrecer el nombre, dígitos y claves de acceso a nuestra información bancaria. Lo que puede derivar en fraudes y que se conozcan nuestros datos bancarios.

- Ofrecer un correo electrónico es un cauce habitual de descarga de virus, que pueden dañar nuestros equipos o hackear nuestra información personal. Además de descargar e instalar aplicaciones de software que envíen correos a nuestros contactos o entrar en nuestro propio equipo accediendo a toda nuestra información.

- Los buscadores registran y almacenan toda la información que buscamos, obteniendo perfiles de conducta y conociendo toda nuestra navegación.

- Nuestro Smartphone disponen de un sistema de geolocalización e información muy personal que se vincula a internet o entra en redes wifi de las que desconocemos su seguridad. Además de permitir a distintas aplicaciones o redes sociales el acceso a la información personal.

La información es poder, y a diario se publica información relevante e incluso perjudicial para algunas personas en internet. Con este nuevo paradigma de la comunicación, los datos que hasta hoy han sido considerados privados para la persona y que pertenecen a un espacio de intimidad, se incluyen en el Big Data.

En cuanto una persona navega a diario por internet o dispone de redes sociales, este espacio privado se ve considerablemente mermado, dado que muy pocos gestionan la privacidad de sus perfiles, no cuidan la información que se publica de ellos mismos y estos datos en muchas ocasiones son prácticamente públicos y están al alcance de cualquiera con una simple búsqueda. Además, en muchas ocasiones los propios sujetos son conscientes al aportarlos, o de manera inconsciente, permiten el uso y la cesión a terceros de estos datos cuando para utilizar una aplicación aceptan los "Términos y condiciones de uso" de la misma.

Haciendo un poco de recorrido por algunos usos habituales de la sociedad actual en internet, vemos como existen muchos más datos sobre las personas en el Big Data. En algunas ocasiones, se piensa que buscadores como Google, o la red social Facebook, conoce nuestros gustos y preferencias por el registro que se queda almacenado en el ordenador cuando hacemos alguna búsqueda. Pero el Big Data va mucho más allá, dado que registra nuestro comportamiento en cada web, determinando nuestros intereses, en función del tiempo en el que estamos navegando por una web concreta, o las noticias que leemos en medios de comunicación digitales. También analiza las marcas que nos gustan, aquellas a las que seguimos y damos a *"me gusta"* en una red social, e incluso lo que estamos deseando comprar, cuando comparamos distintos productos o buscamos en foros relacionados.

Además, cuando vinculamos un buscador como Google con una cuenta de correo Gmail, que es de la misma empresa, ya se conoce: Nombre, apellidos, fecha de nacimiento, teléfono móvil y ubicación. Curiosamente, en smartphones con un sistema operativo *"Android",* para poder disfrutar del mismo, debemos vincular nuestra cuenta Gmail al configurar el teléfono. Dado que es preferible obtener datos y una información completa, no sólo utilizando nuestras búsquedas desde un ordenador, sino también las que hacemos desde nuestro smartphone o tablet. Si seguimos esta línea, Google conoce dónde queremos viajar, por nuestras búsquedas, y si hemos llegado a hacerlo porque registra el sitio desde donde nos conectamos por la geolocalización del smartphone. Se conoce también si estamos en búsqueda activa de empleo o queremos cambiar de trabajo, si buscamos y nos registramos en webs de recursos humanos. Y si vamos más allá pude conocer también el estado de ánimo cada día, en función de las listas de reproducción y música que se escucha en YouTube, que también está vinculado a una cuenta de Google.

Del mismo modo, Google a través de servicios gratuitos como Google Analytics, ofrece a las empresas la posibilidad de conocer el comportamiento de sus consumidores en su sitio web, sin identificar a las personas, pero ofreciendo una gran cantidad de datos relevantes que posee de los usuarios.

Según la Política de Privacidad de Google, aprobada en 2016, dice así: *"Compartiremos tus datos personales con empresas, organizaciones o personas físicas ajenas a Google si consideramos de buena fe que existe una necesidad razonable de acceder a dichos datos, utilizarlos, conservarlos o revelarlos"*, además determina que: *"Podemos compartir información de carácter no personal de forma pública con nuestros partners, entre los que se incluyen editores, anunciantes y sitios web relacionados"*. Aunque también detalla que se pueden modificar los datos que se proporcionan, pero que esto impediría el uso del servicio de forma plena.

Por tanto, nos encontramos ante un nuevo paradigma de comunicación, revolucionado por las nuevas generaciones que han cambiado el uso de la información y su acceso a ella. Y, por consiguiente, han modificado el concepto que se tenía sobre datos personales y la protección de datos. Lo que supone que debe existir un cambio en la regulación de todo lo relacionado con el ámbito de Internet y la información, que esté actualizado a todas las novedades que hemos expuesto. Poco a poco se van aprobando leyes y regulaciones, pero hay que tener en cuenta que deben tener un carácter global e internacional, ya que Internet no tiene fronteras y lo regulado en un país puede diferir de las leyes de otros.

5.3.3 Derecho al Olvido

Actualmente es algo habitual hacer búsquedas de información de personas, a través de motores como Google, para conocer distintos aspectos de su vida que puedan estar en Internet. También, en múltiples manuales de reciente publicación, se conoce el término reputación online, como algo de uno mismo que debemos cuidar y trabajar, para que cada vez que se busque nuestro nombre aparezca aquello que nos interesa que se encuentre. La subida de datos constantes por parte de un usuario o de terceros que aluden a una persona en concreto, propicia que el usuario considere que exista información comprometida de uno mismo en la red y pueda perjudicarle en algún aspecto familiar o laboral.

Según Artemi Rallo, antiguo Director de la Agencia Española de Protección de Datos, *"Son cada vez más voces que reclaman la necesidad de límites y dotar al ciudadano de mecanismos de garantía, principalmente cuando se tratan informaciones no difundidas, ni relacionadas con ellos".*

Recientemente surge el problema, cuando existen denuncias de particulares al propio motor de búsqueda, aludiendo a que existe información privada, que se considera una intromisión de su intimidad, que aparece con una simple búsqueda de un nombre propio. Es en algunas ocasiones una imprudencia del usuario, pero en la mayoría de los casos suele tratarse de una publicación o difusión de una información publicada por un tercero. Por ello el Tribunal de Justicia de la Unión Europea en 2014, hizo pública una sentencia en la que se recoge que los datos que se muestren deben cumplir unas leyes de protección de datos, y que el propio usuario puede solicitar que se eliminen los enlaces de cierta información perjudicial que aparezca, si se cumplen una serie de requisitos.

Este derecho hace posible que se evite la difusión de datos, fotografías, vídeos e informaciones, que puedan perjudicar algún derecho fundamental de una persona. Así como eliminar de los buscadores alguna información obsoleta, falsa, u obtenida de forma ilícita que sea perjudicial para el usuario. Para que esto se realice debe ser una información que cumpla unas especificaciones determinadas o que haya sido publicada de forma ilícita. Es decir, aquella información que no sea de relevancia pública, o que haya sido obtenida de forma que vulnere el secreto de las comunicaciones. Incluso aquellas informaciones que estén amparada por los derechos de libertad de información o libertad de expresión, en algunos casos.

Cuando te ampara este derecho, la información no se elimina de la fuente inicial. Lo que se hace es impedir su difusión en una escala global, al no aparecer en el motor de búsqueda. Ya que puede ser un proceso judicial u otro en función de la circunstancia de la publicación o de la propia información en sí. Ya que puede ocurrir el caso de que la información sea subida por un tercero. En este caso, el responsable es quién lo sube a la red, pero en un proceso penal se debe investigar a todas aquellas personas que lo difunden.

5.3.4. - Libertad de Información y Libertad de Expresión en Internet

La libertad de información es un derecho fundamental que recoge la Constitución Española en el artículo 20 del Título I, que reconoce y protege el derecho:

"A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades."

Por un lado, la libertad de información permite difundir libremente aquella información veraz, que cumpla una mínima diligencia profesional, que se haya obtenido de forma lícita, y que tenga relevancia pública. Se protege también cuando la información es publicada por cualquier soporte o medio de comunicación con cierta solvencia y repercusión. Todo cambia cuando el auge de internet hace que perfiles de particulares asuman este derecho de libertad de información, a través de las redes sociales, blogs, o comentarios.

Dado que no está especificado qué soporte o medio es el que debe protegerse o no, se ha creado así el periodismo ciudadano, formado por usuarios aleatorios que informan sobre temas de actualidad y ejercen una profesión periodística paralela al interactuar en la red.

Por otro lado, en el ejercicio periodístico coexiste la libertad de información, con la libertad de opinión, que viene recogida en el mismo artículo y es conocida como la libertad de expresión: *"A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción."*

Es difícil desvincular una libertad y otra en el ejercicio de la profesión periodística, ya que después del dato objetivo, puede encontrarse un análisis subjetivo. No obstante, estos derechos son los que permiten a los periodistas ejercer su profesión amparados por un derecho fundamental, siempre y cuando no vulneren otros derechos fundamentales. Tal y como viene especificado en el mismo artículo: *"Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia."*

En el periodismo en especial, se suceden multitud de demandas por la intromisión de un derecho de libertad de información o de libertad de expresión, que se enfrentan a derechos al honor, intimidad o a la propia imagen.

5.3.5. - Derecho al Honor, a la Intimidad y Propia Imagen.

- Derecho al Honor.

Como hemos comentado anteriormente, se trata de otro Derecho Fundamental recogido en el Artículo 18 de la Constitución. Este derecho trata de proteger la buena reputación de la persona, penando expresiones o mensajes públicos que supongan un menosprecio o descrédito de la persona. Salvaguardando la reputación y consideración que se tenga de una persona en un grupo social, o la que tenga sobre sí misma de su ámbito personal, familiar o laboral.

El Código Penal español, tipifica como delito las injurias *"la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación"* y las calumnias *"la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad"*. Los derechos de libertad de expresión e información, chocan a menudo en redes sociales contra este derecho al honor.

Teniendo en cuenta que esta protección del derecho del honor tiene una parte objetiva y otra totalmente subjetiva, hay que considerar que puede producirse una imprudencia del usuario ofendido, que ha dado lugar a comentarios despectivos, existiendo así una

responsabilidad propia del usuario que denuncia. En el caso de que sea un desprecio producido por un tercero la responsabilidad es del usuario infractor. Aunque podríamos decir que el amparo de un usuario ofendido, en ocasiones es atacado por un usuario falso, que encuentra en internet confianza para cometer delitos y acusaciones, a través de un ordenador y una identidad fraudulenta. Lo que dificulta su búsqueda y pena, y por consiguiente una tardía rectificación de lo comentado. Esto puede ser mucho más perjudicial cuando hablamos de que ha sido una empresa la atacada, lo que recuperar su honor es mucho más complicado.

- Derecho a la Intimidad.

Asimismo, el Derecho a la Intimidad es un Derecho Constitucional amparado por el Artículo 18. Este derecho protege la esfera más íntima de un individuo, así como resguardar la dignidad humana de una persona. Lo que el Artículo 18 garantiza, es el secreto sobre ese ámbito de nuestra vida personal, y por ello veta a terceros a hablar y publicar informaciones sobre este contorno privado de cada persona.

En las redes sociales, es constante la vulneración de este derecho cuando se publica información ajena, algo que se observa en fotografías, vídeos, comentarios o información que no tiene el consentimiento de hacerse público de todos los protagonistas del contenido. Creando en muchas ocasiones daños y perjuicios con consecuencias que pueden llegar a ser penales. Pero claro, el dilema surge cuando se enfrentan dos derechos; libertad de expresión y de derecho a la intimidad. Si un particular siente que se han vulnerado alguno de sus derechos por la información que publica en una red social o un medio de comunicación digital, puede interponer una demanda civil o incluso una denuncia por la vía penal, al medio de comunicación, al periodista que firma, o al usuario que hace la publicación. En este caso entrarían a debate, por ejemplo, si un usuario con un perfil público y un número considerable de publicaciones que se consideran que entran en su ámbito íntimo, puede denunciar una publicación porque contra su intimidad, o si se considera que un usuario con muchos seguidores tiene “relevancia pública”.

Pero con la vorágine del ámbito digital, toda la legislación se vuelve difusa. Dado que como es algo novedoso, se puede llegar a entender que existe un delito, pero no el

proceso o la vía judicial que se debe tomar, dado que actualmente se está trabajando en los reglamentos que lo especifiquen.

- Derecho de Propia Imagen.

Se entiende como el Derecho de propia imagen a la titularidad y protección de cada persona de su imagen, impidiendo su difusión para la obtención de algún beneficio sin su consentimiento. Por tanto, un tercero no puede captar nuestra imagen, reproducirla y publicarla, pretendiendo así que cada individuo decida qué desea que se haga público con su imagen. Todo esto se agrava si el uso de una imagen ajena es utilizado para un beneficio comercial y no se tiene el consentimiento del propietario de los derechos de esa imagen.

Aquellas redes sociales que utilizan la subida de imágenes como parte fundamental de su actividad, tienen intrínseca en su uso la cesión de derechos de propia imagen de cada usuario que se da de alta en la red social, en los términos y condiciones de uso que se acepta al registrarse en la misma. Cediendo todos los derechos de imagen de todas aquellas fotografías que se suban a la red social. Podemos encontrarnos varias circunstancias que tendrían una resolución totalmente diferente. Dependiendo de la red social, se tendrán unos derechos de imagen u otros, hay algunas en las que se pierden los derechos de imagen por completo y en otras en los que hay ciertas limitaciones o restricciones.

Por ejemplo, Facebook permite que un tercero comparta fotografías, sin consentimiento, siempre y cuando sea siempre dentro de la misma red social. Utilizando su herramienta de *"compartir"*, pero nunca utilizando la fotografía como si fuera propia, en otro ámbito o subiéndola desde otro perfil que no tenga permiso. Esto implica que se pierden todos los derechos de imagen frente a la red social Facebook, pero no frente a un tercero, ya que en ningún caso podrá guardar una fotografía de la red y utilizarla para algún beneficio comercial, sin autorización expresa del propietario.

Además, la propia red social permite determinar, cada vez de una forma más exhaustiva, quiénes son las personas que pueden ver o no las fotografías que se suban.

Evitando así que se pueda llegar a considerar que el propio usuario no valora sus derechos al honor, intimidad y propia imagen porque el contenido que sea público de un perfil pueda ser perjudicial para la persona, sin que ésta sea consciente que todo es público y puede afectarle. Otro caso fraudulento del derecho de propia imagen sería el uso de las mismas, para enriquecer un perfil falso en internet.

- Insultos y sentencias a favor de aquellos que demandan por perfiles desconocidos.

Según la Memoria Anual de la Fiscalía (2015), se registraron en 2014 más de 20.000 procesos judiciales de delitos en Internet. En lo que concierne a delitos relacionados con los derechos fundamentales recogidos en el Artículo 18, han aumentado de forma sustancial por el elevado uso de las redes sociales en la sociedad. Ejercer el derecho de libertad de expresión en redes sociales con un uso poco responsable de las mismas, puede derivar en un proceso judicial que puede resolverse a través de la vía civil, con una indemnización para el afectado por parte del que realiza la publicación. Pero hay casos en los que se dan circunstancias que pueden llegar a la vía penal.

Encontramos un problema sustancial cuando el perfil que atenta contra algún derecho fundamental anteriormente nombrado, es un perfil "desconocido", es decir, que utiliza un nombre de usuario falso y un correo electrónico que no identifica a la persona. Estos perfiles pueden ser denunciados en las propias redes sociales para que se inhabiliten las cuentas, pero hasta que no existe una demanda formal contra este usuario, la policía no puede investigar quién es el responsable de las acusaciones públicas vertidas online.

Actualmente existen muchos procesos judiciales derivados de estos delitos de redes sociales que suelen solucionarse por la vía civil, ya que tampoco existen unos criterios específicos para solucionarlos, dado que dependen mucho las circunstancias. Pero es interesante la sentencia del Tribunal Supremo del 13 de julio de 2016, que hace referencia al caso del usuario de Twitter Madame Guillotine, que publicó unos mensajes humillantes hacia víctimas del terrorismo como Irene Villa o Miguel Ángel Blanco.

En esta sentencia se hace alusión a que existen ciertos mensajes que no pueden enmarcarse dentro de la libertad de expresión dado que están cargadas de odio.

Especificando también que con esta sentencia no se trata de coartar la libertad de expresión, sino de "combatir actuaciones dirigidas a la promoción pública de quieres ocasionan un grave quebranto en régimen de libertades y daño en la paz de la comunidad con sus actos". Esta sentencia supone un cambio existencial en los distintos procesos que puedan estar actualmente abiertos con causas semejantes, dado que se induce a penar el enaltecimiento del terrorismo en este caso.

Aunque tras esta sentencia también se podría abrir el abanico a casos relacionados con el acoso escolar, promoción de la anorexia o la bulimia o humillaciones desproporcionadas. Como las sucedidas tras la muerte del torero Víctor Barrio, en las que la red se incendió de críticas y comentarios alegrándose de su fallecimiento por el hecho de ser torero.

Del mismo modo suceden otros casos conflictivos por ejemplo el que el Tribunal Superior de Justicia de Castilla la Mancha el 8 de abril de 2016, en el que se consideró procedente el despido a un trabajador por publicar en Facebook una serie de comentarios ofensivos de carácter sexual, hacia dos compañeras de trabajo. Una muestra de cómo los comentarios publicados en las redes sociales pueden ser motivo de un conflicto entre trabajadores y empresa.

Por éstos y otros miles de casos que saltan a la parrilla de la actualidad haciendo alusión a conflictos y delitos relacionados con el mal uso de Internet y las redes sociales, es necesario comentar la importancia de la imagen personal y profesional que se proyecta en el ámbito digital.

Y para terminar este punto cuarto, debemos recordar que el derecho penal una de las respuestas que el Estado ofrece para mantener el orden y la convivencia pacífica. Internet y las nuevas tecnologías, citando nuevamente a Alejandro Puerto Mendoza, poseen un gran potencial para lesionar gravemente y afectar directamente a la paz y el orden público necesarios para la adecuada convivencia y el desarrollo social.

En base a lo anterior el estado lucha contra la “cibercriminalidad” bien con medidas represoras, centradas en la respuesta penal a las conductas más graves, bien mediante medidas de seguridad preventiva contra los posibles ataques intencionados.

La popularización del uso de Internet ha hecho que el número de actuaciones ilícitas sea muy amplio, y se encuentran además en continuo cambio, por lo que su calificación jurídica dentro de la tipificación realizada por la ley penal puede llegar a ser muy difícil.

5.4. Redes Sociales

Aun siendo conscientes de todo ello de una forma superficial, la tecnología e internet están tan vinculados a nuestra vida diaria que, casi de forma involuntaria, todos interactuamos en el ámbito online de tal forma, que afecta a nuestras decisiones y estilo de vida en el ámbito offline. Existe una necesidad y un afán constante por hacer público todo lo que hacemos en nuestro día a día, nuestros logros y éxitos, así como dejar claras nuestras opiniones y gustos en redes sociales.

Según el estudio de Interactive Advertising Bureau (IAB), Asociación de la Publicidad, Marketing y Comunicación Digital, junto con VIKO, Grupo de empresas de Marketing Digital, el 82 % de los internautas españoles entre 18 - 55 años utilizan redes sociales de una forma habitual. Esto quiere decir que 14 millones de internautas de nuestro país utilizan las redes sociales en su día a día. La red social Facebook, sigue siendo por excelencia la más utilizada por los usuarios, con un promedio de uso de 6 días por semana. Lo que supone que la red social está integrada en la sociedad actual. Este uso tan normalizado que se hace para estar presente en internet, conocer información de las marcas y estar en contacto permanente con nuestros amigos y conocidos, hace necesario detenerse en un análisis, de ciertos aspectos de las redes sociales más utilizadas en España.

Es importante conocer que Facebook e Instagram se rigen por la normativa de privacidad estadounidense y Twitter por la estadounidense y por la irlandesa. Únicamente el gigante Google, se adapta a las normativas de cada país en el que se establece.

Aunque es evidente y ya se ha mencionado anteriormente, aceptamos y firmamos un contrato virtual de términos y condiciones de uso de las redes sociales, obligatoriamente para poder registrarnos y utilizar el servicio. Dando nuestro consentimiento a una serie de cláusulas que muy pocos se molestan en leer, dado su lenguaje consultivo, jurídico y una pésima traducción al español.

Prácticamente todas las redes sociales rehúsan su responsabilidad en el caso de abrirse un proceso judicial, por un conflicto derivado del mal uso de las plataformas. Suelen aludir a que lo que cada uno publica, es su responsabilidad. Y en el caso de que lo haga un tercero, hay que responsabilizar al que lo haya publicado. Incluso Facebook impone unas *"reglas de uso"*, para implicar al usuario en hacer un correcto uso de la plataforma.

Hay que tener en cuenta que, en un proceso judicial derivado de un conflicto, adquiere mucho peso para la toma de decisiones respecto a una sentencia, el uso habitual que le dé un usuario a sus redes sociales. Por ello, en cuarto lugar, hay que tener un uso responsable de las mismas, en cuanto a subir fotografías seleccionadas, que no puedan perjudicarnos ni que den demasiada información de nuestra vida personal.

Y en último lugar, relacionado con las fotografías, hay que ser conscientes de los datos que se proporcionan a estas plataformas. Como sabemos, lo habitual es facilitar nombre, apellido, correo electrónico o teléfono móvil al registrarnos. Pero lo más interesante de las redes sociales son los contactos con los que se nos relaciona, y la información que ofrecemos por el uso habitual de una red social, como pueden ser: marcas a las que seguimos, comentarios, *"me gusta"* a ciertas publicaciones o búsquedas.

Esta sería la información que utilizan las redes sociales para elaborar perfiles de cada uno de los usuarios que ofrecen a los anunciantes, sin identificar por completo a las personas. Los anunciantes pagan por hacer campañas publicitarias en las redes sociales. Éstas serán más efectivas y tendrán un retorno rentable cuanto más cerrado esté el target de lo que ofrecen. Para estas campañas se seleccionan con todo lujo de detalles los perfiles de usuarios ideales, para ofrecer el producto de la marca. Desde datos físicos, como el género, edad, ubicación o nivel académico, hasta datos relacionados con los gustos, aficiones y pasiones. Toda esta información que está en línea es muy complicada eliminarla por completo, ya que aunque se elimine el perfil que las subió a la red, si otro usuario lo ha compartido es casi imposible borrar el rastro.

Analizaremos a continuación los aspectos de cada red social (más utilizadas) que pueden perjudicar nuestra marca personal.

5.4.1- Facebook.

Es la red social que establece unos criterios complejos de privacidad a elección del usuario. Es decir, se puede seleccionar si se desea que las publicaciones sean públicas, si se quiere que solo la vean amigos, incluso si se quiere que la publicación la vea una persona o un grupo reducido. Aunque hay que tener en cuenta, que por mucho que se bloqueen usuarios para que no vean ningún contenido, o no se acepten las peticiones de amistad, el problema no es lo que publica uno mismo, sino también, las publicaciones que otros usuarios relacionan con un perfil, mediante etiquetas, menciones o comentarios.

Hay que tener en cuenta que la foto de perfil y la foto de portada, siempre son públicas. Es bueno que se reconozca a la persona con cierta facilidad, para poder explotar al máximo el uso de la red social. Pero, por otro lado, hay que considerar que debe ser decente y coherente con la imagen que se desee proyectar. En Facebook existe una opción en los criterios de privacidad que se llama *"revisión de la biografía"*. Esta opción, permite al usuario seleccionar si se desea que aparezcan o no todas las publicaciones que se quieran colocar en una biografía, las imágenes en las que se le etiquete o incluso comentaros en los que se le mencione. Esto debe activarse, al igual que se deben revisar todos los criterios de privacidad, como, por ejemplo, que pueda buscar un perfil por el teléfono móvil, o por el correo electrónico. Algo que, si queremos ocultar un perfil con un cambio de nombre, pero está vinculado a nuestro correo habitual, es incoherente.

También, puede llegar a ser perjudicial lo que comentamos por la red social o a las fotografías a las que le damos a me gusta. Eso se debe a que una de las últimas actualizaciones de la red social permite a los amigos, o de forma pública si no está especificado, que aparezca en el timeline de quién nos hacemos amigos, qué comentamos en una publicación, o a que foto le hemos dado a me gusta. Además, a los contactos del usuario les aparece claramente que ese contenido aparece en su timeline porque su amigo ha interactuado con él. Por lo que el uso responsable de la red social va más allá de únicamente considerar lo que publicamos o no.

En esta red social, es en la que más descarado se ha visto el uso de la publicidad, ya que la encontramos tanto integrada en el contenido de forma sutil, como, por ejemplo, especificado que son anuncios en los laterales. El criterio que se utiliza para que veamos unos anuncios u otros, es el que surge del pago de los anunciantes por campañas publicitarias. Estas marcas eligen al perfil al que desean que les aparezca el anuncio, y Facebook lo hace.

La red social se caracteriza por tener una gran plataforma gratuita de estadísticas que especifican cuantas personas lo han visto, a cuántas les ha podido llamar la atención porqué han interactuado con el anuncio, o cuántas han llegado al objetivo pretendido con las publicaciones.
Y las marcas que tengan una fan Page pueden acceder fácilmente a estas estadísticas e ir controlando tanto sus publicaciones, como sus campañas publicitarias, analizando siempre al público que sigue sus contenidos. Además de que en la red social se pueden observar también anuncios que derivan de nuestras búsquedas en Google, ya que incluso nuestra navegación y las cookies se identifican para un uso comercial.

El uso de Facebook es gratuito, porque otros se encargan de darle rentabilidad a nuestra información, aunque la red social mencionará siempre que es para la mejora de la experiencia del servicio. Está claro que no se identifica claramente a ningún usuario, pero si se conectan todos los datos que puede llegar a poseer la red sobre un usuario, prácticamente se sabe toda la información personal de un individuo, y lo más importante, se conocen sus contactos.

Siguiendo esta línea, en sus términos y condiciones de uso se especifica que por tener el perfil activo se hace una cesión de los derechos de imagen y la información obtenida de un perfil se utiliza para análisis de la plataforma. Aunque se menciona que podrá ceder esta información a las marcas que pertenezcan al grupo empresarial de Facebook.

5.4.2.- Instagram.

Desde que pertenece al grupo empresarial de Facebook, comparten prácticamente todos los términos y condiciones de uso, además de las políticas de privacidad. Pero esta red social no permite tanta especificación en cuanto a quién puede o no ver las publicaciones. O es un perfil público o es un perfil privado. Con sus consiguientes datos obtenidos al registrar un perfil en la red social, como el nombre, el correo electrónico, edad, sexo o ubicación. Es curioso que, si se ofrece el número de teléfono, damos a la red social acceso a nuestra agenda personal, o si vinculamos la cuenta de Facebook e Instagram también se notifica quienes de tus amigos tienen un perfil en la otra red social. Lo primero suena más escalofriante, porque lo consideramos más íntimo y lo segundo se considera algo normal. Cuando desde un punto de vista objetivo, es lo mismo.

En esta red social al igual que en Facebook, las campañas de los anunciantes funcionan igual, ya que incluso se permite que se relacionen las dos plataformas en la misma campaña para obtener más impacto. Y la cesión sutil para los anunciantes en forma de perfiles con características físicas y otras más complejas, al igual que la información que se ofrece a otras empresas del mismo grupo es idéntica a: *"Empresas que sean legalmente parte del mismo grupo empresarial de la marca"*.

El usuario también cede los derechos de las imágenes que se suban a Instagram, y se hace especial alusión a que cada uno es responsable de lo que se publica y se establecen algunos contenidos que pueden ser censurados por la marca. Pero volvemos a lo mismo, el responsable es el usuario que sube la imagen a la red, sea propio o sea un tercero, pero la red social se desvincula de cualquier responsabilidad que pueda derivar de un conflicto.

Pero en esta red social lo interesante es como se obtiene rentabilidad del uso habitual de la misma, con la información que se va aportando día a día. Todo esto en una amalgama de datos cruzados de hashtag utilizados, tipos de fotografías subidas, el contenido de las mismas, los datos del registro del perfil, los que se obtienen por el uso de Facebook, los seguidores, los seguidos, incluso las búsquedas de Google, hacen que se ofrezcan unos contenidos u otros en la pestaña de *"explora"*. No contentos con todo esto, también se registra la interacción que se tengan con los usuarios y esto puede

ser visto por nuestros seguidores o seguidos. Por ejemplo, si un usuario comenta una fotografía, a alguno de sus seguidores que tenga sus mismos intereses, puede aparecerle esta imagen en su pestaña *"explora"*. Además, le aparece la imagen y el comentario del usuario, por lo que imaginemos que es una fotografía que por algún motivo pueda comprometer al usuario, y uno de sus seguidores es su jefe, su uso irresponsable hace que pueda tener problemas.

5.4.3.- Twitter.

En esta red social al igual que en Instagram, o es un perfil público o es un perfil privado. Además, los buscadores suelen posicionar el perfil de Twitter en uno de los primeros puestos si se hace una búsqueda de una persona. Y esta red social es conocida por los tweets imprudentes derivados de un momento de tensión, que dejan su rastro en la red. Por lo que se debe evitar en su uso diario los comentarios que puedan perjudicar al usuario. Un dato curioso de los términos y condiciones de uso de Twitter es que ofrecer el número de teléfono es opcional, pero en el caso de que se aporte se consiente la recepción de mensajes publicitarios al móvil. O también, aunque no se especifique, la red social se vincula con el GPS del smartphone concretando una ubicación, aunque no se publique expresamente donde estamos. Del mismo modo, la rentabilidad de esta red es el uso de sus consiguientes datos obtenidos al registrar un perfil, así como los obtenidos por el contenido publicado, seguidores, seguidos, retweets o favoritos. Además de que otros usuarios pueden revelar información personal con menciones, que puede ser dañina para un usuario.

Lo curioso también de esta red, es la alusión en sus términos y condiciones de uso a la cesión de los datos públicos aportados en el registro del perfil y los derivados del uso de la red social para hacer "deducciones" sobre cómo mejorar experiencia de los usuarios o de la plataforma.

6.- METOGOLOGÍA PRÁCTICA

6.1. Metodología

De acuerdo con la Guía sobre "Privacidad y Seguridad en Internet", elaborada como publicación conjunta por la Agencia Española de Protección de Datos, AEPD, y el Instituto Nacional de Ciberseguridad, INCIBE, en sus páginas web:
www.agpd.es y www.incibe.es

Internet y los servicios que en la red se prestan se han convertido en imprescindibles en nuestras vidas, pero ello es posible gracias a la ingente cantidad de datos que nosotros mismos facilitamos, lo que conlleva un alto riesgo para nuestra privacidad y seguridad, del que, en numerosas ocasiones no somos conscientes.
El objetivo de esta breve encuesta es saber precisamente hasta qué punto somos conscientes de los riesgos que corremos al facilitar nuestros datos a través de la red, y si sabemos protegernos adecuadamente.

Preguntas realizadas:

1.- ¿Tienes cuentas personales con acceso a través de Internet, como, por ejemplo, correos electrónicos, redes sociales u otros perfiles? Si/No
2.- ¿Qué tipo de perfiles o plataformas utilizas?
- Google.
- Facebook.
- Instagram.
- Twitter
- LinkedIn.
- Otro.

3.- El riesgo de pérdida o robo de nuestro dispositivo móvil siempre existe. ¿Tienes protegido su acceso mediante bloqueo de pantalla con código numérico o patrón? Si/No
4.- ¿Utilizas redes wifi públicas?: Si/No

4.1.- Si has respondido Si a la pregunta anterior, en esos casos, ¿intercambias información privada o confidencial, como datos bancarios etc.?: Si/No

5.- ¿Utilizas las mismas contraseñas de acceso a los distintos servicios que usas, como Facebook, Gmail, Instagram, a pesar de que sabes que no es una buena práctica? SI/No
6.- ¿Has utilizado alguna vez una capa de seguridad extra a las contraseñas, de forma que para acceder a tu cuenta sea necesario además de usuario y contraseña, un código? Si/No
7.- ¿Haces copia de seguridad de los datos almacenados en tus dispositivos? Si/No
8.- ¿Utilizas servicios de Banca on-line? Si/No
9.- ¿Haces compras on-line? Si/No
10.- ¿Lees los términos y condiciones de uso de las distintas aplicaciones para conocer los derechos que tienes a la protección de tus datos personales? Si/No
11.- ¿Revisas con frecuencia la configuración de tus perfiles de privacidad en las distintas redes sociales para asegurarte de quien puede ver lo que publicas? Si/No
12.- ¿Subes fotos con frecuencia a tus redes sociales? Una vez a la semana/Mas de una vez a la semana /Menos de una vez a la semana.
13.- ¿Utilizas los servicios de almacenamiento de datos de alguna nube? Si/No
14.- ¿Cuál es tu edad?
15.- ¿Sexo? Hombre/Mujer
16.- ¿Estudios Universitarios? No/Si
Se han realizado estas preguntas de forma on-line utilizando la plataforma de encuestas a través de formularios que nos facilita la cuenta de Gmail de Google, y la distribuiremos entre todos nuestros contactos a través de la aplicación de mensajería en línea WhatsApp.
Utilizamos esta metodología porque consideramos que es la mas adecuada a los objetivos de información para el análisis del comportamiento y evolución por tramos de edades, que pretendemos conseguir.
La herramienta metodológica utilizada es el análisis cuantitativo, que es aquel que busca establecer la cantidad de algún elemento presente en una muestra.

6.2. Análisis de Resultados

Una vez lanzada la encuesta entre un universo de 500 usuarios de todas las edades y condiciones, hemos obtenido respuesta on-line de 260 usuarios, lo que supone un 52% de respuesta, lo que consideramos suficientemente significativo para analizar los resultados obtenidos y establecer conclusiones.
Vamos a analizar las respuestas a cada pregunta de forma porcentual:

1.- ¿Tienes cuentas personales con acceso a través de Internet, como, por ejemplo, correos electrónicos, redes sociales u otros perfiles?

El 98,8% ha respondido que SI.

Esto coincide con el Estudio Anual de Redes Sociales de España de 2017, que establece que el 86% de la población española (19,2 millones) entre 16 y 65 años utilizan redes sociales.

2.- ¿Qué tipo de perfiles o plataformas utilizas?

- Google. Han respondido que SI el 91,9%
- Facebook. Han respondido que SI el 73,1%
- Instagram. Han respondido que SI el 47,7%
- Twitter Han respondido que SI el 25,4%.
- LinkedIn. Han respondido que SI el 37,3%. La encuesta pone de manifiesto que esta red profesional esta adquiriendo mucho auge en los últimos tiempos.
- Otro. Suponen menos del 1%.

3.- El riesgo de pérdida o robo de nuestro dispositivo móvil siempre existe. ¿Tienes protegido su acceso mediante bloqueo de pantalla con código numérico o patrón?

El 78,5% han respondido que SI y el 21,5% que NO.

4.- ¿Utilizas redes wifi públicas?:

El 57,7% ha respondido que SI y el 42,3% que NO.

4.1.- Si has respondido Si a la pregunta anterior, en esos casos, ¿intercambias información privada o confidencial, como datos bancarios etc.?:

El 80% ha respondido que NO y el 20% que SI.

Estas preguntas se han realizado con la intención de conocer si existe una preocupación real sobre la protección de datos personales que podemos tener en nuestros dispositivos móviles. La preocupación existe, pero tras los resultados de la pregunta 4.- constatamos que la mayoría de la muestra tiene cuidado a la hora de ofrecer datos sensibles como pueden ser los bancarios, pero no tanto en los datos personales ofrecidos en el momento de registrarse en una red social, que de acuerdo con la pregunta 1.- tienen el 98,8% de los usuarios.

5.- ¿Utilizas las mismas contraseñas de acceso a los distintos servicios que usas, como Facebook, Gmail, Instagram, a pesar de que sabes que no es una buena práctica?

El 63,8% ha respondido que NO y el 36,2% que SI

6.- ¿Has utilizado alguna vez una capa de seguridad extra a las contraseñas, de forma que para acceder a tu cuenta sea necesario además de usuario y contraseña, un código?

El 75,4% ha respondido que NO y el 24,6% que SI.

Volvemos a constatar con estas 2 preguntas que existe una conciencia social, pero que a la hora de llevarla a la practica no se toman las suficientes medidas de protección.

7.- ¿Haces copia de seguridad de los datos almacenados en tus dispositivos?

El 60,4% ha respondido que SI y el 39,6% que NO.

La mayoría de la muestra protege de forma personal sus datos, por lo que le dan importancia al contenido que puedan tener en un dispositivo móvil, y les preocupa la pérdida de esa información.

8.- ¿Utilizas servicios de Banca on-line?

El 82,3% ha respondido que SI y el 17,7% que NO.

9.- ¿Haces compras on-line?

El 80,8% ha respondido que SI y el 19,2% que NO.

En estas dos preguntas entendemos que se confía plenamente en las aplicaciones usadas porque se facilitan datos muy sensibles sin ningún tipo de filtro. Estas respuestas demuestran un exceso de confianza que puede ser peligrosa.

10.- ¿Lees los términos y condiciones de uso de las distintas aplicaciones para conocer los derechos que tienes a la protección de tus datos personales?

El 81,5% ha respondido que NO y el 18,5% que SI.

En mi opinión, esta es la pregunta mas importante relacionada con la hipótesis general del trabajo, es decir, existe una realidad con respecto al desconocimiento de la legislación vigente que regula todo el contenido digital.

11.- ¿Revisas con frecuencia la configuración de tus perfiles de privacidad en las distintas redes sociales para asegurarte de quien puede ver lo que publicas?

El 60,4% ha respondido que NO y el 39,6% que SI.

El objetivo principal de este trabajo es concienciar sobre la importancia de la autorregulación y la prudencia frente a la publicación de contenidos en la red. Por tanto, podemos concluir que mas de la mitad de la muestra, no revisa la privacidad de sus contenidos digitales, por lo que se hace necesaria la educación y conciencia social en este sentido.

12.- ¿Subes fotos con frecuencia a tus redes sociales?

Una vez a la semana: El 11,5%

Mas de una vez a la semana: el 9,2%

Menos de una vez a la semana: El 79,2%

13.- ¿Utilizas los servicios de almacenamiento de datos de alguna nube?

El 56,9% han respondido que SI y el 43,1% que NO.

Existe ya un 20% de la población que publica de forma habitual contenidos en redes sociales. Esto es un dato muy importante que está relacionado con la tendencia futura del uso generalizado de las redes, y almacenamiento de datos en la nube.

14.- ¿Cuál es tu edad?

Rango de edades:

- Menos de 25 años: 8,08%
- 26-35 años: 31,92%
- 36-45: 11,92%
- 46-55: 9,23%
- 56-65: 31,92%
- 66-75: 6,15%
- Mas de 76 años: 0,77%

15.- ¿Sexo?

Han respondido un 67,3% de mujeres y un 32,7% de hombres.

16.- ¿Estudios Universitarios?

De las respuestas, el 88,5% de los usuarios tienen estudios universitarios y el 11,5% no.

Incorporamos como Anexo el documento Excel completo generado por la plataforma de Google.

7. Conclusiones.

De acuerdo con lo establecido en la "Introducción al Derecho de Internet" (Alejandro Puerto Mendoza, Madrid 2015), la aparición de Internet ha provocado múltiples consecuencias en todos los ámbitos, y el mundo del Derecho no ha sido una excepción. Muchas de las actuaciones desarrolladas en la red son inéditas para el Derecho, el cual no ha podido adaptarse todavía a esta realidad cambiante.

Nos encontramos ante una realidad en la que la labor reguladora pública no ha conseguido todavía la estabilidad y seguridad jurídica deseable en la red.

Frente a esta realidad nos encontramos que, tan importante como la labor reguladora pública es la labor autorreguladora privada. Ambas coexisten, ya que, junto a aun conjunto de leyes, reglamentos, tratados y acuerdos internacionales, existe una regulación privada que se manifiesta por medio de códigos de conducta, reglamentaciones técnicas, usos y buenas costumbres, y otras reglas fruto de la autorregulación que son tan importantes y necesarias como las anteriores.

Y es aquí el momento de hacer una reflexión sobre el título, irónico, con el que hemos bautizado este trabajo: **"Términos y condiciones de uso en Internet: La Normativa es inútil sin la autorregulación del usuario."**

De nada sirve que las administraciones tanto nacionales como europeas se esfuercen en crear y mejorar el cuerpo legislativo disperso, heterogéneo, incompleto y fragmentado que existe actualmente, si a la vez no crece una conciencia social que nos eduque a hacer un buen uso de internet y todas sus derivadas: las redes sociales, las apps, el e-mail, haciendo un uso responsable de los datos personales que volcamos ingentemente en estos medios sin tener realmente conciencia de las consecuencias que para nuestros derechos fundamentales puedan tener estas acciones.

Y de nada sirve que las administraciones y organismos nacionales y europeos se esfuercen en protegernos, y defendernos de los delitos que puedan derivarse de acciones cometidas en este ámbito contra nosotros, si en la raíz de estos delitos cometidos se encuentra una acción u omisión realizada por nosotros en el uso, o, mejor dicho, en el mal uso de los medios informáticos que tenemos a nuestro alcance.

8. MEMORIA

8.1. ELECCIÓN DE LA TEMÁTICA DE LA INVESTIGACIÓN

La elección de esta investigación surge a partir del conflicto que se produce en el uso de las redes sociales en generaciones de usuarios entre 20 - 25 años. Estos usuarios utilizan las redes sociales en un ámbito personal, compartiendo contenido para amigos o conocidos, y sin filtrar los receptores de esta información. Llega un momento en el que estos usuarios entran en procesos de selección en un ámbito laboral, y es aquí cuando surge la preocupación sobre los contenidos que pueden ser perjudiciales para su imagen. Sin embargo, el hecho de que las empresas puedan acceder de forma rápida a esta información que está en línea, hace que aquel que no esté en redes sociales pueda llegar a generar desconfianza.

En este punto, consideramos interesante una investigación sobre la concienciación de los usuarios sobre el contenido que cada uno publica, y las repercusiones legales que pueden surgir de esta información que está en línea. Es una realidad el desconocimiento generalizado por parte de los usuarios en cuanto a términos y condiciones de uso de las redes sociales, o derecho y deberes que pueden vulnerarse en ámbito digital. El usuario ofrece datos personales a redes sociales, aplicaciones, registros en línea y compras en comercio electrónico, sin tener en cuenta el uso que se hace de los mismos por parte de estas empresas.

La legislación vigente está obsoleta, partiendo de la base de que en primer lugar, debe haber una normativa global que abarque todos los aspectos que engloba internet. Es decir, el hecho de que internet sea utilizado de forma indiferente por usuarios ubicados en países distintos y la información almacenada en servidores por todo el mundo; hace que la legislación sea muy compleja. Y en segundo lugar, el uso de las nuevas tecnologías crece de forma exponencial sin que existan calificaciones jurídicas para la casuística que se puede producir.

Por tanto, es aún más relevante la necesidad de concienciar a los usuarios que utilizan internet de forma habitual, sobre el uso que hacen estas aplicaciones con los datos personales que ofrecen. Además de las analíticas e informes de comportamiento que se realizan con la información que se encuentra registrada en los servidores o Big data.

8.2. PROPUESTAS DE CONTINUACIÓN DE INVESTIGACIÓN

1. El hecho de que se nos ofrezcan multitud de servicios gratuitos con el uso de estas aplicaciones y redes sociales en internet, se basa por un lado, en la publicidad personalizada que se nos ofrece; en función del uso que hacemos de internet. Y por otro lado, el uso que hacen estas empresas con los datos personales y de comportamiento que registran estas empresas de los usuarios.

2. La indeterminación en las distintas calificaciones jurídicas de los delitos que surgen por las publicaciones en línea, por culpa de la cantidad de factores que intervienen en cada caso. Es decir, no se han especificado las actuaciones que pudieran dar lugar a hechos punibles, ni la normativa penal ha desarrollado los elementos a tener en cuenta para que constituyan un delito.

3. Un estudio social sobre la conciencia en el uso de las redes sociales y las nuevas tecnologías en las generaciones jóvenes y las más maduras. La realidad sobre la adaptación de las generaciones maduras en las redes sociales y la prudencia sobre la intimidad en comparación con el uso habitual de éstas por las generaciones jóvenes. Ya que los jóvenes no consideran que aportar ciertos datos personales sean una intromisión en su intimidad.

4. Derecho de Libertad de Expresión en ámbito digital en contraposición a los Derechos Fundamentales de Honor, Intimidad y Propia Imagen en la red. Internet ha propiciado que se vulneren estos derechos de forma consciente o inocente, ya que no se tiene una educación sobre los límites aplicables en la red. En esta línea de investigación sería interesante abordar la autorregulación del usuario, para evitar estas situaciones.

5. Estudio y análisis de los términos y condiciones de uso de las redes sociales. Ya que la redacción de éstos se encuentra disponible para todos los usuarios, sin embargo, suele tener una traducción confusa, un lenguaje consultivo y jurídico , que complica la comprensión del lector. Esto genera un desconocimiento sobre la regulación de una aplicación que tiene un uso diario por parte del usuario.

8.3. TENDENCIAS

Lo más inmediato, en lo que se está trabajando tras esta investigación es en las nuevas regulaciones globales, que se adapten a la realidad actual del uso de las nuevas tecnologías.
Es el ejemplo del nuevo 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. Una norma directamente aplicable en los países miembro que está vigente en España desde el 25 de mayo de 2018, y que obliga a las empresas a llevar a cabo las actuaciones que especifica.

Otra tendencia que se irá desarrollando a lo largo del tiempo, es el cambio del uso de las redes sociales entre las distintas generaciones. Facebook comenzó siendo una red social para compartir contenido con amigos y conocidos, se extendió hasta tener un uso generalizado por la sociedad en todo tipo de rangos de edad, aunque actualmente es una de las redes que más intervención tienen por parte de la publicidad y las marcas.

9. REFERENCIAS BIBLIOGRÁFICAS

9.1. Libros

- AGUADO TERRÓN, J. M. & MARTÍNEZ RODRÍGUEZ, L. (2005). *Introducción a la comunicación periodística escrita*. Murcia: Diego Marín.
- AGUSTINO Y GUILAYN, A. & MONCLÚS RUIZ, J. (2016). *Aspectos legales de las redes sociales*. Barcelona: Bosch.
- MEJIDE, R. (2014). *Ubrands*. Barcelona: S.L.U. Espasa Libros.
- ORDÓÑEZ SOLÍS, D. (2014). *La protección digital de los derechos en Internet en la Jurisprudencia Europea.* Madrid: Editorial Reus.
- PUERTO MENDOZA, A. (2015). *Introducción al Derecho de Internet. Régimen Jurídico básico de los contenidos digitales*. España: Centro de Estudios Financieros.
- SANJURJO, B. (2015). *Manual de Internet y Redes Sociales*. España: Dykinson. S.L.
- SERRANO MARÍN, V. (2016). *Fraudebook*: *lo que la red social hace con nuestras vidas*. Madrid: Plaza y Valdés.

9.2. Vídeos documentales

- *Documentos TV: Big Data: Conviviendo con el algoritmo*, 2017. Madrid: Televisión Española (TVE). Disponible en: http://www.rtve.es/alacarta/videos/documentos-tv/documentos-tv-big-data-conviviendo-algoritmo/3893978/
- *Documentos TV: Disparates en Facebook*, 2017. Madrid: Televisión Española (TVE). Disponible en: http://www.rtve.es/alacarta/videos/la-noche-tematica/noche-tematica-disparates-facebook/3291998/
- *Documentos TV: Ojo con tus datos*, 2013. Madrid: Televisión Española (TVE). Disponible en: http://www.rtve.es/alacarta/videos/documentos-tv/documentos-tv-ojo-tus-datos/2270048/

9.3. Artículos en Prensa

- AGUDO, A. “Internet lo sabe (casi) todo sobre usted”. *El País*, [en línea] 18 de Marzo de 2013. Sección (Vida & Artes). Página 32. Disponible en: https://elpais.com/sociedad/2013/03/17/actualidad/1363555505_736818.html
- CONSEJO DE LA UNIÓN EUROPEA, 2017. “La UE reforzará la ciberseguridad”, [en línea], 20 de noviembre de 2017. Disponible en: http://www.consilium.europa.eu/es/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/
- EFE, 2017. “El Supremo prohíbe publicar sin permiso fotografías tomadas de Facebook”. *El Correo de Andalucía*, [en línea], 20 de febrero de 2017. Disponible en: http://elcorreoweb.es/espana/el-supremo-prohibe-publicar-sin-permiso-fotografias-tomadas-de-facebook-FA2673135
- GARCÍA CAMPOS, J.M. “El tesoro de los datos masivos”. *La vanguardia*, [en línea] 8 de noviembre de 2013. Disponible en: http://www.lavanguardia.com/magazine/20131108/54392775355/big-data-datos-masivos-reportaje-en-portada-magazine-10-noviembre-2013.html
- JIMÉNEZ, B. “Telefónica vende los datos de sus 44.000.000 de clientes a Inditex”. *Ok diario*, [en línea] 10 de marzo de 2017. Disponible en: https://okdiario.com/economia/empresas/2017/03/10/telefonica-vende-datos-44-000-000-clientes-inditex-817781

9.4. Documentos electrónicos

- AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO. (2016). *Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.* [en línea]. Dirección: https://www.boe.es/doue/2016/119/L00001-00088.pdf [consulta: agosto de 2018].
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2016). *Guía del Reglamento General de Protección de Datos para Responsables de tratamiento*. [en línea]. Dirección: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf [consulta: agosto de 2018].
- COMISIÓN EUROPEA. (2015). *Una Estrategia para el Mercado Único Digital de Europa*. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*. [en línea].

Dirección: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&from=ES [consulta: agosto de 2018].

9.5. Páginas WEB

- EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, 2018. [en línea]. Disponible en: https://www.europol.europa.eu/es/about-europol [consulta: agosto de 2018].
- FACEBOOK, 2018. *Condiciones del Servicio*. [en línea] Disponible en: https://es-es.facebook.com/legal/terms [consulta: junio de 2018].
- GOOGLE, 2018. *Privacidad y Condiciones*. [en línea] Disponible en: https://policies.google.com/terms?hl=es-419 [consulta: junio de 2018].
- INSTAGRAM, 2018. *Condiciones de uso*. [en línea] Disponible en: https://es-la.facebook.com/help/instagram/478745558852511 [consulta: junio de 2018].
- INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2018. [en línea]. Disponible en: https://www.incibe.es/ [consulta: julio de 2018].
- OFICINA DE SEGURIDAD DEL INTERNAUTA, 2018. [en línea]. Disponible en: https://www.osi.es/es [consulta: julio de 2018].
- THE EUROPEAN UNION'S JUDICIAL COOPERATION UNIT, 2018. [en línea]. Disponible en: http://www.eurojust.europa.eu/Pages/languages/es.aspx [consulta: agosto de 2018].
- TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, 2018. [en línea]. Disponible en: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_es [consulta: julio de 2018].
- TWITTER, 2018. *Términos de Servicio* [en línea] Disponible en: https://twitter.com/es/tos [consulta: junio de 2018].