UNIVERSIDAD MIGUEL HERNÁNDEZ

Facultad de Ciencias Sociales y Jurídicas de Elche

INTIMIDAD, PROTECCIÓN DE DATOS Y FACEBOOK

TRABAJO DE FIN DE GRADO

Autor: Manuel Antonio Gutiérrez Navarro

Tutora: Rosario Tur Ausina

Grado en Derecho

2022

ÍNDICE

ABREVIATURAS.

C.E.	Constitución Española
EEUU	Estados Unidos de América
F.J.	Fundamento Jurídico
FB	Facebook
FTC	Federal Trade Commission / Comisión Federal de Comercio
IA	Inteligencia Artificial
IG	Instagram
ISP /ISP's	Internet Service Providers
L.O.	Ley Orgánica
MI	Machine Learning/Aprendizaje Automático
R.A.E.	Real Academia Española
RGPD	Reglamento General de Protección de Datos
RRSS	Redes Sociales
STC	Sentencia Tribunal Constitucional España
TJUE	Tribunal Justicia de la Unión Europea
UE	Unión Europea

1. INTRODUCCIÓN.

La aparición en nuestras vidas de los smartphones y las redes sociales[1] [en adelante RRSS] nos ha abierto un mundo de posibilidades inimaginable hace unos años. Pero ese mundo de posibilidades también está lleno de peligros que afectan directamente a nuestros derechos fundamentales.

El aparente acceso gratuito a servicios y plataformas, a cambio de soportar un poco de publicidad, es el cebo usado por esos "proveedores de servicios" o "Internet Service Providers ISP's" en terminología anglosajona. La cruda realidad es que no son gratuitos. El precio somos nosotros, nuestros datos, datos que entregamos gratuitamente para que sean recolectados, almacenados y analizados según dicen para ofrecernos un contenido "adaptado a nuestros gustos y preferencias[2]"

El ser humano es una máquina generadora de datos, información susceptible de ser analizada. Nuestra identidad es un cúmulo de características físicas, culturales, psicológicas, económicas, etc. que nos definen y nos hacen diferentes a los demás, un conjunto de atributos de naturaleza cuantitativa y cualitativa que tienen valor económico para empresas e instituciones. Si ese ingente volumen de datos personales lo combinamos con la enorme capacidad de análisis de datos, en cantidad y calidad (media en términos de capacidad de predicción), que permiten las nuevas tecnologías desarrolladas en los últimos 30 años, como la inteligencia artificial "IA" o el "Machine Learning [ML], nos encontramos ante una auténtica amenaza para nuestra intimidad.

Parece, por tanto, lógico preguntarse ¿qué datos entregamos?[3], ¿hasta dónde llega esa cesión de datos?, ¿somos conscientes de lo que hacemos?, ¿qué ocurre con ellos?, ¿quién o quiénes los tienen?, ¿dónde los tienen?, ¿hasta cuándo los tienen?, ¿qué conocimiento extraen de ellos?. Son preguntas cuyas respuestas tal vez nos sorprendan y disgusten. A alguna de éstas daremos respuesta en las siguientes páginas.

---

[1] Aunque en este TFG hacemos referencia solo a las redes sociales y específicamente a Facebook. La información contenida en cuanto al uso de datos y al comportamiento monopolístico es también aplicable a las GAFAM y BAT. Las grandes empresas tecnológicas norteamericanas son conocidas como **GAFAM**: Google-Amazon-Facebook-Apple-Microsoft, mientras que el grupo de grandes empresas chinas es conocido como **BAT**: Baidu-Alibaba-Tencent.

[2] https://www.facebook.com/legal/terms/update. (Fecha consulta 30/05/2022)

[3] En la exposición de motivos de la L.O. 5/1992 de 29 octubre ya advierte "*El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad en efecto, a una amenaza potencial antes desconocida*".

El objetivo general de este TFG es poner de manifiesto la limitación que la legislación actual, en materia de protección de datos, tiene para la defensa del derecho fundamental a la intimidad y especialmente, el papel relevante de las redes sociales como Facebook. La vigente legislación adopta la concepción del dato como una "variable stock", como una mercancía, algo estático y cuantificable, cuando lo relevante para el ciudadano/usuario es, en mi opinión, la información que se extrae de esos datos (visión dinámica) una vez analizados y, sobre todo, las consecuencias que esa información obtenida post-análisis pueda tener en sus derechos. Un dato, un valor o una cualidad contiene información, pero tiene más si se puede poner en relación con otros que permitan su comparación, valoración y correlación. Lo relevante no es el dato en sí, sino la capacidad de predicción que tienen.

El deseo o aspiración de una persona de hacer algo, de conseguir algo, sea lo que sea ese "algo", está dentro de su esfera privada, de su intimidad. Ese anhelo es algo íntimo, que forma parte de su capacidad de decisión que puede verse influenciada por "los proveedores de servicios" con muchas y variadas técnicas. La capacidad de predicción de los algoritmos le permiten detectar la predisposición del individuo a hacer algo antes de que el propio individuo sea consciente de ello y eso es una intromisión en su intimidad. Parece que hemos pasado del mero análisis de datos a la inducción de conductas.

Esta capacidad de predicción es solo una de las aristas del poliedro que es la ciencia de datos. Otra cuestión, no menos relevante, son los sistemas de toma de decisiones automatizados y la categorización del usuario en segmentos (grupos de usuarios/consumidores que tienen características homogéneas y comunes), y qué ocurre cuando algunas de esas características se alejan de la media. A modo de ejemplo; dos personas con la misma solvencia patrimonial, el mismo nivel de ingresos y con el mismo endeudamiento, tienen la misma capacidad de pago (están en el mismo segmento). Si solicitaran un préstamo a una entidad financiera[4] y la cuota mensual resultante está dentro de su capacidad de pago ésta concedería la financiación. Pero, qué ocurre si dándose las mismas circunstancias, el sistema de análisis de riesgo de crédito tuviera en cuenta más factores (variables cualitativas), p.e. en qué tipo de supermercados suele comprar el cliente (el banco conoce el dato por el uso de la tarjeta de crédito) o que la nacionalidad de origen de uno de los solicitantes fuera de un determinado país (que conoce por obligación legal

[4] Un ejemplo de uso de datos que son conocidos por las entidades financieras. https://www.elgoldigital.com/caixabank-utiliza-datos-privados-de-sus-clientes-para-hacer-estudios-de-salarios/ (Fecha consulta 28/05/2022)

"KYC"). Si el sistema (scoring)[5] ha determinado que los compradores de una cadena de supermercados o con determinada nacionalidad de origen tienen una "experiencia de impago" superior a la media, el resultado será que el cliente verá denegado su préstamo. Este es un claro ejemplo de vulneración del derecho a la igualdad.

Para la redacción de este TFG he tomado como referente del análisis del comportamiento de usuarios mediante algoritmos y otras tecnologías a la red social FACEBOOK por varias razones. En primer lugar, por tratarse de la decana[6] de las redes sociales. Fue fundada en 2004, tres años antes del lanzamiento del primer smartphone. En segundo lugar, y consecuencia de su carácter pionero, porque desde su creación ha tenido que ir solventando diferentes problemas que sus innovaciones han provocado en la privacidad de sus usuarios. En tercer lugar, por ser la red social más importante en número de usuarios con casi 2.910 millones[7] y en cuarto y último lugar porque, en mi opinión, se ha convertido en un monopolio. Su crecimiento en número de usuarios y facturación ha sido exponencial pero no se ha debido sólo a razones endógenas. Durante este tiempo ha crecido mediante adquisiciones de otras importantes redes sociales como Instagram [en adelante IG] en 2011 por unos 1.000 millones de euros y la aplicación de mensajería instantánea WhatsApp en 2014 por otros 14.000 millones de euros. También ha comprado otras compañías como OCULUS VR, desarrolladora de realidad virtual, la israelí ONAVO y en 2020 GIPHY famosa por la creación de imágenes GIF. Hasta 2019 FB había adquirido casi 70 empresas.

Sorprende que todas estas compras no hayan tenido reparos importantes por parte de las autoridades que velan por la competencia, tanto estadounidenses como europeas. Esta cuestión sería también un buen tema para desarrollar en un TFG ya que los reguladores (americanos y europeos) han errado al interpretar cual es el modelo de negocio de FB y no es "el espacio publicitario" que vende a sus clientes, sino la recolección de datos, su análisis y su capacidad de predicción del comportamiento de sus usuarios. Esta "miopía" solo muestra lo difícil que es definir con certeza cual modelo de negocio/producto de las "compañías tecnológicas".

---

[5] Scoring: Sistema automático de evaluación de solicitudes de crédito.

[6] Facebook no fue la primera red social. Cuando fue creada ya existía otra red social denominada "MySpace". https://myspace.com/

[7] Datos obtenidos en https://es.statista.com/estadisticas/600712/ranking-mundial-de-redes-sociales-por-numero-de-usuarios/#:~:text=Facebook%20encabezaba%20de%20nuevo%20en,red%20social%20ha%20sido%20imparable (Fecha consulta 26-05-2022).

Cuando la Federal Trade Commission (Comisión Federal de Comercio) [FTC en adelante] revisó la compra de Whatsapp en 2014, FB alegó que era una simple aplicación de mensajería instantánea y no un competidor directo. De igual modo, planteó la misma estrategia en 2019 cuando compró Instagram, alegando que era una aplicación para compartir fotos y no un competidor directo. Tanto IG como WhatsApp no tenían publicidad en aquel momento. Los reguladores ignoraron la verdadera naturaleza de la actividad de FB permitiendo un nivel de concentración sin precedentes. A más usuarios, más datos, más capacidad de análisis y predicción y más capacidad de influencia.

No ha sido hasta diciembre de 2020 cuando la FTC interpuso una demanda[8] contra Facebook acusándola de ejercer monopolio y de estar realizando prácticas anticompetitivas. En su acusación alega que FB ha desarrollado una estrategia anticompetitiva comprando competidores e imponiendo condiciones a los desarrolladores de software.

ESTRUCTURA

El presente TFG está divido en tres bloques. Un primer bloque donde trataré el derecho a la intimidad en internet que indudablemente no puede desligarse del derecho al honor y a la propia imagen. También abordaré aquí el uso de algunos conceptos que son utilizados erróneamente de forma sinónima pero que tienen naturaleza y significado distinto. Y seguidamente, la influencia que las Redes Sociales [en adelante RRSS] acaban teniendo en nuestra vida privada, sus implicaciones y riesgos. Por último, en este apartado, veremos la percepción del riesgo que la exposición pública en las RRSS tiene o puede tener en la vida de los usuarios.

La segunda parte de este bloque tratará la naturaleza del dato, cual ha sido su evolución de la ciencia de análisis de datos, su valor, y como ejemplo de todo ello, el uso de las "cookies" por las páginas web y que suponen por sí mismas una fuente de información esencial para terceros.

El segundo bloque está destinado al análisis de la RRSS hegemónica: Facebook. Veremos sus orígenes, evolución, qué servicios presta, qué datos recopila y cuál es su

[8] https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization (Fecha consulta 13/06/2022)

política de uso y privacidad y valoraré si sus algoritmos pueden limitar de alguna forma nuestra libertad de elección.

En la segunda parte veremos cual es la normativa vigente sobre protección de datos personales nacional y europea, cuál ha sido su evolución y la regulación actualmente en desarrollo por parte de la Unión Europea. También qué derechos en materia de protección de datos tienen los ciudadanos y cómo ejercerlos.

Finalmente, en el tercero y último bloque daré las razones por las cuales la actual normativa me parece insuficiente para la defensa del derecho a la intimidad de las personas y propondré algunas medidas que sería razonable adoptar para fortalecer la capacidad de decisión, por parte de los usuarios, sobre sus datos personales.

2. DERECHO A LA INTIMIDAD E INTERNET

Con carácter previo a tratar el derecho a la intimidad en las próximas páginas es necesario abordar la diferente concepción que de este derecho hay en Europa y en EEUU Esta es una cuestión esencial que, como se verá más adelante, ha generado cierta beligerancia política entre ambos lados del Atlántico y explica muchas de las controversias que "los proveedores de servicios" han tenido en Europa a cuenta de su legislación, mucho más garantista.

En Europa, el derecho a la intimidad tiene un respaldo constitucional. La Carta de Derechos Fundamentales de la Unión Europea[9] recoge en su art. 7 el derecho a la intimidad, "Respeto a la vida privada y familiar", y en su art. 8 contempla el derecho a la "protección de datos de carácter personal". También es recogido en las Constituciones nacionales de los Estados miembro de la UE[10].

Sin embargo, en EEUU se utiliza un enfoque distinto, un enfoque sectorial que se basa en una combinación de legislación, regulación y autorregulación. El derecho a la intimidad

[9] Carta de los Derechos Fundamentales de la Unión Europea. Texto Completo. https://www.europarl.europa.eu/charter/pdf/text_es.pdf (Última consulta 30-05-2022)

[10] La UE y los EEUU han firmado varios acuerdos relativos al tratamiento de datos de ciudadanos europeos en los EEUU Dichos acuerdos han sido ratificados por los países que forman parte de la UE así como Noruega, Islandia y Liechtenstein que forman parte del Espacio Económico Europeo (EEE.). Suiza no forma parte de éste pero sí de la Asociación Europea de Libre Comercio (AELC) y firmó un acuerdo bilateral con EEUU Para saber más: https://www.europarl.europa.eu/factsheets/es/sheet/169/el-espacio-economico-europeo-suiza-y-el-norte

no se menciona en su Constitución. No obstante, en la jurisprudencia constitucional si ha surgido una interpretación de este derecho. Allí este derecho se basa en la Primera Enmienda[11] y en la protección de la Quinta Enmienda contra la autoincriminación, así como la protección de la Cuarta Enmienda contra los registros del gobierno cuando un individuo tiene una "expectativa razonable de intimidad"[12]. El Tribunal Supremo reforzó el derecho a la intimidad en 1965 articulando la existencia de una "zona de intimidad" protegida del individuo, que posteriormente ha aplicado en decisiones relativas a particulares sobre sexo, salud y sobre revelaciones de secretos de estado.

Las regulaciones específicas sobre el tratamiento de datos y su protección siempre han contado con gran oposición política primando sobre el derecho a la intimidad, la seguridad, la libertad de expresión o la iniciativa económica. Solo es posible encontrar normativa sobre protección de datos en ámbitos específicos como la salud o las finanzas. La norma más importante sobre protección de la privacidad es la "Privacy Act[13]" de 1974. Esta ley se aplica al control de datos por parte de organismos federales y exige la notificación real, la publicación y la compatibilidad del uso con el propósito para el que se recogió. Su funcionamiento no es como el de una ley global como lo hace el Reglamento General de Protección de Datos [en adelante RGPD] europeo, p.e. no regula la transferencia de datos desde los "proveedores de servicios" al gobierno aunque si regula la transferencia a otros agentes privados.

En EEUU es la Comisión Federal de Comercio (Federal Trade Commission FTC) el principal órgano encargado de velar por la privacidad de los datos y cuya misión esencial es "proteger a los consumidores y promover la competencia"[14]. Su actividad se centra en la persecución de prácticas mercantiles engañosas y desleales respecto al uso de datos por parte de las empresas, sobre todo si esas prácticas causan un perjuicio sustancial a los consumidores que no es compensado por beneficios a consumidores o a la competencia.

Esta ausencia de una norma clara sobre protección de datos, al modo europeo, le ha dado una gran importancia a la autorregulación de las propias empresas del sector, en su

---

[11] Constitución de los EEUU Texto completo. https://www.archives.gov/espanol/constitucion (Fecha consulta 30-05-2022)

[12] Katz vs United States. 389 US 347, 360 (1967) https://supreme.justia.com/cases/federal/us/389/347/#:~:text=United%20States%2C%20389%20U.S.%20347%20(1967)&text=It%20is%20unconstitutional%20under%20the,privacy%2C%20unless%20certain%20exceptions%20apply. (Fecha consulta 30/05/2022)

[13] Privacy Act 1974. Texto completo https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies. (Fecha consulta 30/05/2022)

[14] https://www.ftc.gov/es/acerca-de-la-ftc/lo-que-hacemos (Fecha consulta 30/05/2022)

mayoría norteamericanas, obviamente, esa autorregulación en un tema tan delicado ha demostrado ser insuficiente. Una de las limitaciones de la autorregulación es que no tiene capacidad coactiva y, que su uso se basa en la buena fe y el compromiso de su cumplimiento por quienes la han suscrito. Pero, ¿qué ocurre cuando una innovación o un nuevo producto muy rentable está en contra de esas normas?. Este fue el caso de la aplicación lanzada por FB en 2007 llamada "Beacon"[15]. Esa aplicación había sido diseñada para recabar información sobre las compras que realizaban los usuarios (entradas de cine, viajes, etc.) y los publicaba en los "news feed" de sus amigos. Su único inconveniente es que no había recabado el permiso de los usuarios para compartir esa información, lo que provocó su ira contra la compañía iniciando una campaña de recogidas de firmas en MoveOn.org que en pocos días había reunido 50.000 firmas, a las pocas semanas reconoció su error y dio marcha atrás.

En el caso de Europa, el proceso constituyente desarrollado a partir de finales de la segunda guerra mundial e inspiradas en los postulados establecidos en la Declaración Universal de Derechos Humanos de 1946 y en la Convención Europea de Derechos Humanos[16]de 1950, incorporaron definitivamente el derecho a la intimidad como derecho fundamental.

1. ¿Qué es el derecho a la intimidad?

El diccionario María Moliner de Uso del Español define la intimidad como "*un conjunto de sentimientos y pensamientos que cada persona guarda en su interior"*; por su parte el diccionario de la Real Academia de la Lengua define intimidad como la "*zona espiritual íntima y reservada de una persona o grupo, especialmente de una familia*". La palabra intimidad proviene del latín "intimus" que significa lo que está más adentro. Es por ello por lo que la intimidad se entiende "*como un derecho inherente a la persona, que no debe conquistarlo ni para poseerlo ni se pierde por desconocerlo. Más bien se percibe como una característica del ser humano por el hecho de serlo*".

En la Constitución Española de 1978 este derecho está recogido en art. 18, Título I, y dice:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[15] Story, Louise. Facebook retreats on online tracking".
https://www.nytimes.com/2007/11/30/technology/30iht-30face.8538279.html (Fecha consulta 12/06/2022)
[16] Convención Europea de Derechos Humanos. Texto completo.
https://www.echr.coe.int/Documents/Convention_SPA.pdf (Fecha consulta 30/05/2022)

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."

Este artículo fue desarrollado posteriormente mediante 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. En su art. 7. detalla qué actividades tienen la consideración de intromisión ilegítima en la intimidad.

"Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

Uno. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

Tres. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

Cuatro. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

Cinco. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.

Seis. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

Siete. La divulgación de expresiones o hechos concernientes a una persona cuando la difame o la haga desmerecer en la consideración ajena."

Pero, además, la jurisprudencia de nuestro Tribunal Constitucional en varias sentencias ha moldeado y perfilado el concepto de intimidad. Así p.e. en la STC 207/1996, de 16 de diciembre, F.J. 3º, dice *"el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 C.E.), implica 'la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana".* En otra sentencia, STC 115/2000 F.J. 4º dice "*que el derecho fundamental a la intimidad reconocido por el art. 18.1 C.E. tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 C.E.), frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar (STC 231/1988, de 2 de diciembre, y 197/1991, de 17 de octubre), frente a la divulgación del mismo por terceros y una publicidad no querida. No garantiza una intimidad determinada sino el derecho a poseerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 C.E. garantiza es, pues, el secreto sobre nuestra propia esfera de intimidad y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los lindes de nuestra vida privada.* En la STC 73/1982 F.J. 5º dice *"… pues la intimidad es un ámbito o reducto en el que se veda que otros penetren y que no guarda por sí solo relación directa con la libertad de relacionarse con otras personas o derecho a tener amistades, que es a lo que la recurrente parece referirse.".*

Así pues, la intimidad es un ámbito del ser humano inaccesible para el resto, particulares o poderes públicos (facultad de reserva) y vinculado a la dignidad de la persona (STC 209/1988, F.J. 3.° "…*derivación de la dignidad de la persona"*) sobre la que se establece una facultad de disposición respecto a su publicidad y por tanto la posibilidad de controlar además aquello que haya salido de nuestra esfera interna.

En cuanto al derecho fundamental a la protección de datos recogido en al art. 18.4 C.E., éste otorga a sus titulares un poder de disposición y control sobre los mismos que habilita a los ciudadanos el derecho a decidir qué datos comparte y con quién los comparte. En la STC 292/2000 en su F.J. 7º dice "*De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la*

protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".

El filósofo Byung-Chul Han en su libro Psicopolítica afirma[17] "*nuestra vida se repoduce totalmente en la red digital. Nuestro hábito digital proporciona una representación muy exacta de nuestra persona, de nuestra alma, quizá más preciosa o completa que la imagen que nos hacemos de nosotros mismos*" y es esa la razón de la imbricación de los derechos a la intimidad y a la protección de datos. En un mundo digital no puede entenderse el uno sin el otro, insiste Byung-Chul Han "*la vigilancia digital es más precisa porque es aperspectivista*", lo que significa que esa vigilancia a la que somos sometidos es global y no deja resquicio a ángulos muertos (nuestras zonas íntimas). Nuestra intimidad se defiende a través del control de nuestros datos, pero sobre todo, conociendo qué averiguan con ellos quienes los tienen.

2. La intimidad, vida privada y privacidad

Los términos intimidad, vida privada y privacidad son usados habitualmente como sinónimos, y aunque existe cierta conexión entre ellos son conceptualmente distintos. El uso del término privacidad[18] tiene su origen en el derecho anglosajón "Right to privacy". El término "Privacy" aparece en el famoso ensayo publicado por los abogados norteamericanos Samuel D. Warren y Louis D. Brandeis en la revista Harvard Law Review en 1890 y que se convirtió en el referente fundacional de la protección de la esfera privada, entendida como el derecho a "no ser molestado" o "right to be let alone", en definitiva el derecho a estar solo. El sustantivo "Privacy" ha sido incorporado al Diccionario de la Real Academia de la lengua como Privacidad definiéndolo como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

Una buena explicación sobre la diferente sustantividad de los términos privacidad e intimidad la encontramos en la exposición de motivos de la L.O. 5/1992 de 29 de octubre, ya derogada, de regulación del tratamiento automatizado de datos de carácter personal donde "*Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues*

[17] Byung-Chul Han, Psicopolítica, Editorial Herder, Barcelona, 2014. Pág. 93.
[18] La "privacidad" es un neologismo como traducción literal de la palabra inglesa "privacy"

en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo"

La vida privada tiene que ver con la conexión entre la esfera íntima de la vida de un individuo y la esfera pública. El ser humano es un ser social pero esa socialización con el resto es gradual y basada en el grado la confianza que se deposita entre ellos, entendida esta confianza como el nivel de injerencia que se le admite a ese tercero. Así pues, desde la más íntima esfera del individuo hasta la esfera pública existen diferentes grados de intimidad, o dicho de otro modo, un diferente conocimiento de esa intimidad y de lo que ocurre dentro de ellas. Como dice el profesor Martínez de Pisón[19] "*Intimidad, vida privada y lo público son espacios separados pero conectados son Espacios cambiantes en cada momento y situación, hasta tal punto que una misma acción puede considerarse pública, privada o íntima con sólo variar el cómo y el dónde se realiza*". La vida privada es la faceta social de una persona y está referida a aspectos laborales, profesionales o económicos.

3. Redes sociales y vida privada

Las redes sociales se han convertido en una ventana de exposición pública, un escaparate de nuestra vida privada donde compartir sentimientos, opiniones, pensamientos, videos y fotos. Son un espacio virtual de libertad de expresión y de conexión con otros con una audiencia potencial de millones de personas. Ese espacio virtual donde otorgamos una confianza a conocidos y desconocidos con los que compartimos nuestra vida privada se convierte también en el receptáculo que recibe la proyección de nuestra identidad, que aunque digital, sigue contando con los mismos derechos que nuestro yo físico.

a) Implicaciones.

[19] Martínez de Pisón, José. Vida Privada e intimidad: implicaciones y perversiones. Anuario de Filosofía del Derecho XIV. 1997. https://dialnet.unirioja.es/descarga/articulo/142345.pdf

El acceso a la información y el entretenimiento es la principal ventaja de las RRSS aunque no la única. Está permitida la libertad de expresión (sujeta a las normas de uso). Son una herramienta de intercambio de información y conocimientos dada la posibilidad de establecer contacto con personas que comparten las mismas inquietudes que nosotros. Nos ofrecen la posibilidad de hacer negocios y explorar nuevas áreas de conocimiento y nos dan la posibilidad de compartir iniciativas sociales, económicas y políticas.

b) Riesgos.

Además del aspecto lúdico de las RRSS, su uso (indebido) puede comportar riesgos. Como seres humanos tenemos el derecho a equivocarnos pero la proyección mediática que tienen puede suponer que un pequeño desliz o un comentario banal tenga una trascendencia, que en realidad, no tiene o no se desea. Un primer peligro es el riesgo reputacional. Reputación es según el diccionario de la R.A.E. la "*1. Opinión o consideración que se tiene a algo o a alguien y 2. Prestigio o estima que son tenidos a alguien o algo*". Así pues, la ironía no es bienvenida.

En segundo lugar, y relacionado con lo anterior, es la ausencia de contexto, es decir, el desconocimiento del entorno físico, de situación, político, histórico, cultural o de cualquier otra índole en el que se considera un hecho. Se trata de una merma de información que puede hacer que el receptor de una información la malinterprete. En tercer lugar, la publicación de información ajena, ya sean fotografías, vídeos o comentarios sin el consentimiento del afectado. Esta fue una de las circunstancias que, como veremos más adelante, le generó a FB cuando introdujo el etiquetado de imágenes en 2010 innumerables quejas de los usuarios. Debido a las críticas recibidas por parte de los usuarios FB se vio forzada a introducir un mecanismo de autorización de etiquetado a los usuarios de modo que fueran estos, en última instancia, quienes decidieran si se realizaba o no el etiquetado de imágenes. En cuarto lugar, la sobreexposición de datos personales especialmente protegidos. El uso poco prudente de la red puede hacernos publicar circunstancias personales como nuestro estado de salud, convicciones políticas o religiosas.

Otro de los riesgos más importantes es la "falsa sensación de seguridad". Se trata de un entorno virtual y no físico. El ser humano está preparado fisiológicamente para detectar situaciones de peligro inminente. Sin embargo, en un entorno virtual no existe tal percepción del riesgo si no se ha recibido la formación necesaria para detectarlo. En sexto

lugar, el "Uso indebido de datos por terceros". En las RRSS se comparte mucha información personal, a veces de forma imprudente, como p.e. la foto de un DNI, una dirección, un número de teléfono, información que puede ser utilizada por terceros para cometer fraudes, o suplantaciones de identidad. Otro riesgo es la publicación de información falsa. Aquí entra en juego el derecho al honor. La publicación de información falsa o denigrante sobre otra persona afecta a su derecho al honor y puede ser perseguida judicialmente. Pero una cuestión que ha tenido mucha relevancia en las RRSS ha sido la publicación de noticias falsas o "fake news" con el objetivo de influir en la opinión pública. Éstas son noticias esencialmente falsas, que no se ajustan a los hechos, o que han sido adulteradas parcialmente tergiversando hechos generalmente con un objetivo de desinformación, manipulación política, etc. Ejemplo de esto fue el escándalo de la compañía Cambridge Analytica o la campaña electoral de Donald Trump.

Las redes provocan adicción. Su diseño fomenta que los usuarios pasen en ella el mayor tiempo posible, cuanto más mejor. Las redes sociales han copiado lo métodos del juego creando una ansiedad incontrolada aprovechando la "necesidad de validación social", activando los mismos mecanismos cerebrales que las drogas. Si son capaces de crear adicción tal vez sería prudente plantearse la necesidad de que sean objeto de una regulación como la del tabaco.

Otro de los riesgos más importantes de las redes sociales es el "Ciberbulling o Ciberacoso"[20] y el "Grooming". El primero de ellos es el acoso o intimidación que puede sufrir un usuario en las redes cuyo objeto es humillarlo o atemorizarlo difundiendo mensajes o la publicación de fotografías o videos hirientes. El "grooming" es otra forma delictiva de acoso que implica que un adulto contacta con un menor con el fin de ganarse su confianza para luego involucrarle en una actividad sexual.

4. ¿Somos conscientes de los riesgos?

i. Baja percepción del riesgo de exposición

En el apartado anterior hemos expuesto una serie de riesgos que las RRSS e internet tienen. Se trata de una relación no cerrada ni excluyente porque es posible que aparezcan nuevos peligros que actualmente no se han detectado. Lamentablemente no percibimos el

[20] Ciberacoso. UNICEF. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

riesgo que tenemos con nuestro dispositivo y/o perfiles sociales. No somos conscientes de cuánto de nuestra vida privada exponemos.

Una breve encuesta[21] que he realizado con conocidos con cuenta activa en redes sociales ha puesto de manifiesto que es posible encontrar usuarios absolutamente despreocupados por la privacidad (<10%), una gran mayoría que si muestra interés por la privacidad y toma algunas medidas para protegerla (82-83%) y un porcentaje mínimo (7-8%) que se toma muy en serio su privacidad y toma medidas restrictivas. Es una muestra pequeña para poder extrapolar conclusiones al conjunto de usuarios, pero dos conclusiones se pueden extraer; la primera que cada vez se presta más atención al cuidado de la privacidad, qué se comparte y con quién se comparte. Y en segundo lugar, que ese incremento de la atención se produce a raíz de algún inconveniente sufrido en las redes sociales.

Parece que ese comportamiento se ha denominado "La paradoja de la privacidad"[22] y describe la discrepancia entre la actitud del usuario y su comportamiento en relación con la privacidad online, lo que finalmente resulta en una dicotomía entre las actitudes de privacidad y el comportamiento real[23]: los usuarios afirman estar muy preocupados de su privacidad, no hacen nada para protegerla.

3. LA CIENCIA DEL DATO

La protección de nuestros derechos fundamentales debe ser compatible con el ejercicio de la libre empresa recogido en el art. 38 de nuestra Constitución. Las autoridades deben velar por crear entornos que promuevan el desarrollo económico, la prosperidad y dotar de seguridad jurídica el tráfico mercantil. No en vano, el RGPD de denomina "*..a la protección de las personas físicas….y a la libre circulación de esos datos*…" adoptando la idea de que los datos son un bien que puede ser objeto de intercambio comercial y que ese intercambio está sujeto a unas condiciones.

---

[21] Muestra compuesta por 32 personas adultas. Cuestionario de uso.

[22] Barth, Susanne; y De Jong, Menno D. T. "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Elseviers". *Telematics and Informatics,* vol. 34, n.º 7, noviembre de 2017, pp. 1038-1058. TITULO REVISTAS Y TITULO MONOGRAFÍAS EN CURSIVA
https://www.sciencedirect.com/science/article/abs/pii/S0736585317302022 (Fecha consulta 12/06/2022)

[23] Barnes, S.B. "A privacy paradox: Social networking in the United States".
http://firstmonday.org/article/view/1394/1312 (fecha consulta 12/06/2022)

El legislador se ve en el brete de buscar un equilibrio entre el fomento de la innovación y las externalidades negativas que esas innovaciones tienen en los derechos de los ciudadanos. Ese equilibrio no siempre es fácil de mantener puesto que las líneas que separan derechos e intereses no siempre son claras y definidas.

I. Origen y evolución

La mayoría de los profesionales coinciden en establecer como el origen de la ciencia de datos al trabajo realizado por británico John Graunt en el S. XVI. Durante 50 años Graunt registró las causas de la muerte de personas publicados semanalmente por las parroquias y con ellos realizó un estudio concienzudo y novedoso sentando las bases de una herramienta fundamental en el desarrollo de las ciencias como es el análisis de datos.

La "Ciencia de Datos o Data Science" es una disciplina que tiene como objetivo extraer conocimiento a partir de un conjunto grande de datos estructurados en bases de datos o no estructurados (como textos, audios e imágenes) mediante el uso de técnicas estadísticas e informáticas como el análisis exploratorio, el aprendizaje automático (machine learning), el aprendizaje profundo (Deep learning) o la visualización de datos. Los datos son información que se utiliza para encontrar patrones, extraer significado y descubrir conocimiento en base a ello. Esta ciencia, a través del análisis de estos busca obtener respuestas óptimas para, en definitiva, tomar decisiones.

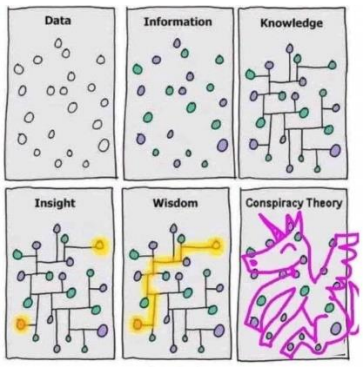


Gráfico 1. Fuente www.mltut.com

La evolución de la actividad comercial en el mundo y la aparición de nuevos competidores en los mercados ha obligado a las empresas a adoptar los sistemas de gestión basados en "data driven decision" – decisiones basadas en datos. La capacidad de

adaptación a la demanda, a los gustos de los clientes, la detección de nuevas preferencias o nichos de mercado no se obtienen por mera casualidad o instinto.

II. Qué es un dato

La primera acepción del diccionario de la Real Academia de la Lengua define como Dato: "*información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivabas de un hecho"*. En nuestro caso nos interesan los "datos personales". El Art. 4.1 del RGPD define "«*datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*. Véase que esta definición dada por el RGPD es una definición amplia pero que no incluye la identificación del dispositivo usado por la persona, aunque la localización sólo puede ser obtenida a través de un dispositivo que previamente se ha asociado a una persona.

Los datos se pueden clasificar atendiendo a infinidad de criterios y en función del tipo de investigación que se vaya a realizar, pero centrándonos en las categorías más adecuadas para los datos personales las clasificaciones serían las siguientes (no son excluyentes):

1. Datos Cuantitativos. Datos Cualitativos.
    a. La edad, el peso, la altura. (datos medibles).
    b. Color de ojos, complexión, estado civil.
2. Datos Activos. Datos Pasivos.
    a. Datos activos: intercambiado directamente por el usuario con la RRSS o un proveedor de servicios.
    b. Datos pasivos: información intercambiada en segundo plano por dispositivos y aplicaciones.
3. Atributos físicos. Atributos acumulados en el tiempo y Atributos designados[24].
    a. Edad, peso, color ojos, etc.
    b. Formación, historial médico, metadatos, estado civil. Son datos que se acumulan en el tiempo y pueden cambiar.

[24] Ver nota anterior.

c. Número del DNI. Número de teléfono, nombre y apellidos. Son datos que le vienen dados al individuo en tanto que no participa de su elección, aunque, evidentemente algunos puedan cambiar a posteriori.

III. ¿Por qué estudiar el comportamiento de los usuarios?

Individualmente un dato, independiente de otros, no es más que un atributo, una cualidad. Permite establecer de entrada una taxonomía, pero su única utilidad es una mera clasificación. Lo realmente relevante en la ciencia de datos son las relaciones entre esos datos, establecer patrones y fundamentalmente ser capaz de predecir el comportamiento futuro. Esta es la clave. Dependiendo del contexto, un dato puede ser insignificante o crucial pero su importancia se incrementa cuando se asocia a un algoritmo.

El análisis de datos[25] sigue un protocolo establecido por fases cronológicas que son las siguientes: En primer lugar, se define el "problema", se trata de concretar qué es aquello para lo que estamos buscando una solución, una respuesta. Una buena definición es esencial. En segundo lugar, se recopila información relevante y se almacena. En tercer lugar, se "limpia" y se transforma para mantener su integridad. Aquí se eliminan datos incompletos o incongruentes. Por seguridad los datos deben ser cifrados. En cuarto lugar, se usan herramientas de análisis de datos para sacar conclusiones; patrones de comportamiento, tendencias y correlaciones[26]. Una vez obtenidas las conclusiones se comunican al "decisor" para que actúe y tome las medidas necesarias para corregir el "problema" detectado.

IV. La valorización de los datos

Los datos son un simple atributo, que puede tener un carácter cualitativo o cuantitativo. Nuestros datos son valiosos desde el punto de vista económico en tanto que sirven para predecir nuestro comportamiento y ese comportamiento supone acciones que tienen trascendencia económica (p.e. adquirir determinado bien o servicio) o política (votar a una formación u otra).

[25] Sistemática establecida en el "Curso de análisis de datos de Google". Disponible a través de la plataforma www.coursera.com (Fecha consulta 12-06-2022)

[26] La correlación es una medida estadística que mide hasta qué punto dos variables están relacionadas y de qué manera. Si la variación de una provoca la variación de otra y si esa variación es en el mismo sentido o en sentido contrario.

El resultado del proceso de análisis de datos ya hemos visto que es la detección de correlaciones o el perfilado del usuario, que es vendido por los ISP como una parte de la experiencia de compra o de un servicio que se ajusta a nuestras necesidades. El valor del dato está relacionado directamente con la publicidad y específicamente con su ROAS. Esto es, el retorno esperado de la inversión publicitaria, sencillamente, cuánto ingresas por unidad monetaria invertida en publicidad. Las redes sociales, en nuestro caso FB es capaz de segmentar de tal manera a sus usuarios que el ROAS que percibe es muy elevado debido a la efectividad de la publicidad en FB.

El valor también se puede medir en términos "Retorno sobre la inversión" o ROI (Return on investment) que es una medida de rentabilidad que se calcula en forma de ratio: (ingresos-inversión)/inversión.

Las empresas han descubierto que cuanto más utilizan los datos más comprenden lo necesario que son para su supervivencia. En su cadena de valor se producen datos entre los que se incluyen los obtenidos de los clientes y de su comportamiento que son utilizados para múltiples finalidades como la mejora del servicio, conocer el "feedback" de productos, la detección de nuevos usos y necesidades, etc.

V. Las cookies[27] como ejemplo

Si hay algo que hacemos todos los días es navegar por internet. Cuando visitamos una página web inmediatamente nos aparece un aviso informativo para aceptar o rechazar el uso de "cookies". Las cookies fueron creadas por el ingeniero informático Lou Montulli en 1994 cuando trabajaba para el navegador "Nestcape". Una cookie es un fichero que se descarga en el ordenador, smartphone o tablet del usuario al acceder a determinadas páginas web para almacenar, recuperar y procesar información (personal) sobre la navegación que se efectúa desde dicho equipo, según establece el art. 22.2 de la LSSI.

Por pereza, por la celeridad de nuestra vida cotidiana o simplemente por desconocimiento aceptamos su uso sin reparar en las consecuencias que ello tiene. Las cookies permiten el almacenamiento en el terminal del usuario de cantidades de datos que van de unos pocos kilobytes a varios megabytes y existen de varias clases en función de la entidad que las gestione y su finalidad.

[27] "Cookie" es una galleta con trozos de chocolate. Parece que se adoptó ese nombre por la analogía al rastro de migas dejado por los protagonistas del cuento infantil de Hansel y Gretel de los hermanos Grimm publicado en 1812. En realidad su nombre adecuado hubiera sido el de "rastreadores".

Las cookies pueden ser varios tipos en función de diferentes criterios de clasificación. Así, en función de quién las gestione tenemos "las propias" que son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado. Las "de terceros" son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies. Estas son muy importantes y son las utilizadas por las RRSS para complementar sus servicios. Según su finalidad, nos encontramos con las "estrictamente necesarias", que son aquéllas que permiten la navegación a través del sitio web, garantizan el correcto funcionamiento del mismo y la utilización de las diferentes opciones o servicios que en él existen. Las cookies "Configuración" son aquéllas que permiten recordar información para que el usuario acceda al servicio con determinadas características que pueden diferenciar su experiencia de la de otros usuarios, como, por ejemplo, el idioma, el número de resultados a mostrar cuando el usuario realiza una búsqueda, el aspecto o contenido del servicio en función del tipo de navegador a través del cual el usuario accede al servicio o de la región desde la que accede al servicio, etc. Las cookies "analíticas o de medición" son aquéllas que permiten el seguimiento y análisis del comportamiento del conjunto de los usuarios del sitio web, incluida la cuantificación de los impactos de los anuncios. En particular, se utilizan cookies analíticas o de medición con la finalidad de: medir el rendimiento del contenido, medir el rendimiento de los anuncios, utilizar estudios de mercado a fin de generar información sobre el público. Y finalmente las cookies "de publicidad comportamental", que son aquellas que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función de este. Estas últimas también son de especial uso por las RRSS ya que les permite categorizar al cliente y segmentarlo.

Por ejemplo, para la web del diario "El Mundo" www.elmundo.es la aceptación de sus cookies le permite al diario y a sus socios con los que comparte información, realizar y conocer todo lo expuesto a continuación:

- Utilizar datos de localización geográfica precisa.
- Desarrollar y mejorar productos.
- Utilizar estudios de mercado a fin de generar información sobre el público.
- Medir el rendimiento del contenido.

- Medir el rendimiento de los anuncios.
- Seleccionar contenido personalizado.
- Crear un perfil para la personalización de contenidos.
- Seleccionar anuncios personalizados.
- Crear un perfil publicitario personalizado.
- Seleccionar anuncios básicos.
- Almacenar o acceder a información del dispositivo.
- Analizar activamente las características del dispositivo para su identificación.
- Almacenamiento y acceso a información de geolocalización para realizar estudios de mercado.
- Almacenamiento y acceso a información de geolocalización con propósitos de publicidad dirigida.
- Compartir tus análisis de navegación y grupos de interés con terceros.
- Enriquecer el perfil con información de terceros.

Pero además advierte "*Si das tu consentimiento para los fines anteriores, también permites que este sitio web y sus socios operen el procesamiento de los siguientes datos: cotejar y combinar fuentes de datos off line, garantizar la seguridad, evitar fraudes y depurar errores, recibir y utilizar para su identificación las características del dispositivo que se envían automáticamente, servir técnicamente anuncios o contenido, y vincular diferentes dispositivos*". A continuación detalla casi 140 "socios" con los que compartirá la información, tu información personal y de tu dispositivo.

Todo esto supone lograr una ingente cantidad de información sobre el usuario, información relevante, como p.e. la localización geográfica sobre la que advierte que "*puede [*la información obtenida*] combinarla con otra que hubiera podido ser recabada previamente, tanto en otros sitios web o aplicaciones como por otros medios"*. El Mundo sabe dónde está su lector. Pero también reconocer el dispositivo que está usando, así como su "i*dentificación*". Vayamos por partes, reconocer qué tipo de dispositivo se está usando permite adaptar la presentación al tamaño de la pantalla, detectar si gira, pero también le permite conocer el identificador único del dispositivo, que viene a ser como nuestro DNI digital. Un identificador que se asocia a nuestro comportamiento, y a nuestro perfil. Hay más, el tipo de dispositivo permite segmentar económicamente al usuario (móvil alta gama vs gama media o baja). Esto es completado con otras variables como hobbies o estilo de vida obtenidas desde las aplicaciones de RRSS.

La localización le permite individualizar la publicidad que recibe el usuario ajustándola a anunciantes de su ámbito geográfico. Además, por medio de las cookies analíticas es posible conocer cómo navega el usuario por la página web una vez que entra en ella ("landing"). De este modo es posible conocer qué noticias lee primero, qué secciones visita con más frecuencia (opinión vs deporte), cuánto tiempo pasa en ellas, etc.

Tampoco se debe olvidar que las cookies fueron una auténtica revolución porque, además de efectuar un rastreo más minucioso, provocó un cambio en el modo en que se hacía publicidad en internet, una publicidad dominada hasta ese momento por "banners" y las odiosas "ventanas emergentes".

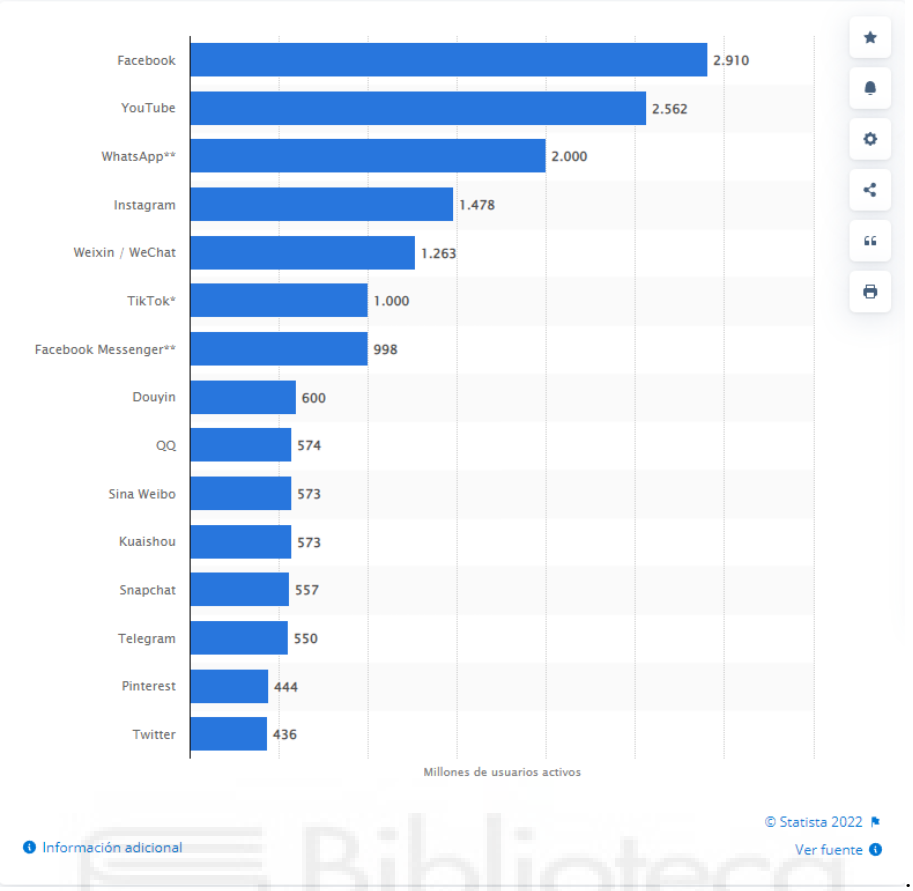
Como vemos, la simple visita a una página web genera decenas de datos que permiten identificar perfectamente al usuario, conocer sus gustos y preferencias, saber dónde está o ha estado. Son datos que se comparten sin que reparemos en su trascendencia y sobre los que podemos ejercer un control que no ejercemos porque no somos conscientes de lo que compartimos

BLOQUE II
REDES SOCIALES Y PROTECCIÓN DE DATOS

4. FACEBOOK. EL NUEVO ORÁCULO

Como mencionaba en la introducción, FB es la red social más importante por número de usuarios y por volumen de ingresos. En 2021 tuvo unos astronómicos ingresos de 117.929 millones[28] de dólares americanos y es la plataforma con mayor número de usuarios.

[28] Fuente: https://es.statista.com/estadisticas/525671/ingresos-mundiales-anuales-de-facebook/#:~:text=Facturaci%C3%B3n%20mundial%20anual%20de%20Meta%20(Facebook)%202010%2D2021&text=Los%20ingresos%20mundiales%20de%20Meta,incremento%20con%20respecto%20a%202020. (Fecha de consulta 30/05/2022)



Cuadro 2. Fuente: es.statista.com

a. **Su origen y desarrollo**

Facebook fue desarrollada por Mark Zuckerberg en 2004 mientras era estudiante en la Universidad de Harvard. Originalmente su nombre era "Thefacebook". En realidad había sido concebida, programada y bautizada por otra persona. Se trataba de un proyecto sin ánimo de lucro destinado a ayudar a los usuarios a localizar a amigos con los que poder contactar.[29]No fue esta primera red social creada por Zuckerberg. Su primera red "FaceMash" tenía un objetivo más primario: poner nota a las compañeras de curso. Éste fue el primer tropiezo con la privacidad de la red. La rápida acogida que tuvo entre los estudiantes provocaron las protestas de las asociaciones de estudiantes femeninas.

En el primer año de existencia alcanzó los 500.000 usuarios y su fundador seguía trabajando en nuevas funcionalidades con el objetivo de que los usuarios pasaran más tiempo en la red; a más tiempo conectado, más información obtienen del usuario. En 2005, FB se había convertido en una de las empresas de las que más se hablaba en Silicon Valley

[29] Frenkel, Sheera y Kankg, Cecilia. Manipulados, Editorial Penguin Random House, Barcelona, 2021. Página 35.

y no solo por el número de usuarios que seguía captando, sino también por la mina de oro que tenía con los datos de sus usuarios.

b. Sus servicios

Para acceder a los servicios de FB solo hay que acceder a su página web www.facebook.com Y hacer clic en "**Crear nueva cuenta"**. En posible crear una cuenta para una persona, un grupo y una "página oficial" (para negocios, empresas o instituciones que cuentan con aplicaciones específicas para publicidad y ventas). En segundo lugar, escribir tu nombre, correo electrónico o número de teléfono móvil, contraseña, fecha de nacimiento y sexo, después clic en "**Registrarte**" y finalmente el paso más importante "confirmar tu dirección de correo electrónico o número de teléfono móvil". Este último paso es importante.

Como veremos más adelante este es uno de los datos esenciales que entregamos y que permite a la compañía una vez instalada la APP propia, conocer qué tipo de móvil tiene el usuario, su geolocalización y otra información que obtiene a partir de aplicaciones que el usuario tenga instaladas en su móvil y que comparten datos con FB. La información que entrega el usuario en el momento del registro se detalla en el siguiente apartado.

c. Facebook como almacén de datos

i. Datos aportados por los usuarios

Los usuarios aportamos los siguientes datos a Facebook:

Información general:	Nombre y apellidos, localidad de nacimiento, lugar de trabajo, dónde has estudiado, lugar de residencia.
Trabajo y formación académica:	Dónde trabajas (se puede informar el nombre de la empresa o institución), universidad e instituto dónde se ha formado el usuario.
Lugares de residencia:	Actual o pasado.
Información básica y de contacto:	Dirección (optativo, pero permite inferir un determinado nivel económico), teléfono (también permite inferir el nivel económico), correo electrónico, página web personal y enlace a otras redes sociales. En cuanto a "información básica": sexo, fecha de nacimiento e idiomas que conoce usuario. También permite incorporar intereses o hobbies, creencias religiosas, e ideología política (estos dos últimos están vedados a los poderes públicos art. 9 L.O. 3/2018).

Familia y relaciones	Situación sentimental y otros miembros de tu familia. (Estos dos factores permiten segmentar al usuario y en función de las interacciones ofrecer publicidad individualizada al grupo familiar)
"Detalles sobre ti":	Pronunciación del nombre, otros nombres (apodo o sobrenombre), y citas favoritas
"Acontecimientos importantes":	Aniversarios, celebraciones, etc.

ii. Datos recopilados por Facebook de los perfiles de los usuarios

La esencia del negocio de FB es la información, y más que la propia información, que es su materia prima, la capacidad de predicción del comportamiento de sus usuarios. No en vano, es líder mundial en "Online Behavioral Advertising", esto es, "Publicidad Conductual en Línea" que implica el seguimiento de las actividades "online" de los usuarios para ofrecerles publicidad personalizada. Y es esta capacidad de predicción la que conculca nuestro derecho a la intimidad porque es capaz de detectar la intención de hacer algo en el usuario antes de que éste sea consciente de ello, de modo que con distintas herramientas puede influir en la voluntad del usuario. De esto, FB no advierte en sus condiciones de servicio, ni en su política de cookies, ni en su política de datos. A continuación veremos cómo capta la información y cómo funciona su algoritmo.

1. ¿Cómo funciona el algoritmo?[30]

El algoritmo funciona a partir de la información aportada por el propio usuario, la obtenida de sus interacciones (Me gusta, estados de ánimo, fotos publicadas[31],etc.), de los textos que escribe (sí, FB lee lo que escribes) y lo aprendido por aprendizaje automático y su inteligencia artificial de las interacciones de millones de usuarios.

Su función es decidir qué publicaciones ven los usuarios cuando se conectan y en qué orden pero también elimina publicaciones que estima no tienen interés para el usuario o directamente éste ha indicado que no le gustan o interesan. Desde su creación, el algoritmo ha evolucionado adaptándose a las necesidades comerciales detectadas por la compañía. En teoría su objetivo es posicionar en el "feed news" (canal de información) aquellas publicaciones que son más relevantes para el usuario. La realidad es otra. FB siempre ha recordado que no existe un único algoritmo sino "*muchas capas del aprendizaje de las máquinas*

[30] https://blog.hootsuite.com/es/algoritmo-facebook-como-funciona/
[31] La inteligencia artificial disponible actualmente permite interpretar el contenido (reconocer caras y objetos) y el contexto de las fotos.

sobre modelos y rankings…"[32]. En 2009 el orden de clasificación de las publicaciones dependía directamente del número de "me gustas". En 2016 priorizó a aquellas publicaciones en las que el usuario pasaba más tiempo. En 2017 cuando introduce las "reacciones" las ponderó más que los "me gusta" y, al año siguiente priorizó las publicaciones que más comentarios recibían con el objetivo de incrementar las interacciones y el tiempo que los usuarios pasaban conectados.

Esto hace que no todos los usuarios accedan a las mismas publicaciones ni en el mismo orden. Se trata de un orden personalizado en función de las preferencias del usuario y sobre todo de los anunciantes. Una vez analizado el algoritmo, veremos seguidamente cuáles son los instrumentos de recogida de información a partir de las interacciones de los usuarios.

2. Me gusta

El "Me gusta" fue incorporado por FB en 2007. Es el detector fundamental de los gustos del usuario. Con un simple click en una noticia, un producto, o un anuncio, le permite a FB conocer con mucha precisión y de modo automático muchas de las características que definen la personalidad de los usuarios. Así es como se alimenta de publicaciones el "News Feed" del usuario. En 2017 incorporó las "reacciones" que su algoritmo pondera más que el "Me gusta". Las reacciones son "*Me encanta, me importa, me enfada, me divierte, me asombra, me entristece*" y se ha convertido en una poderosísima herramienta que permite calibrar el estado de ánimo de los usuarios respecto a una publicación.

Esta aplicación no es más que un continuo test de personalidad que realizamos todos los días millones de usuarios. De este modo FB es capaz de prever comportamientos a estímulos con centenares de variables, el sistema se retroalimenta con IA, interacciones, ML haciendo que las predicciones (comportamiento esperado del "target" al que se le ha dirigido un estímulo) se cumplan.

3. El "news feed"

En las versiones iniciales de FB si el usuario quería ver las actualizaciones de estado de sus amistades debía necesariamente que realizar el esfuerzo de visitar su página personal. En 2006 FB introdujo esta nueva función que se alimenta de las publicaciones, las fotos y las actualizaciones de estado haciendo más fácil su usabilidad y mejorando

[32] Frenkel, Sheera y Kankg, Cecilia. Manipulados, Editorial Penguin Random House, Barcelona, 2021.

considerablemente el flujo de información. Además, incrementaba el tiempo que permanecían conectados y el número de interacciones ya que, a partir de ese momento, son las noticias las que van a su encuentro y no al revés.

4. El etiquetado fotográfico

Otro problema con la privacidad de los usuarios fue la introducción del etiquetado fotográfico en 2007. El etiquetado es una aplicación mediante la cual un usuario que publicaba una foto en FB podía identificar a quienes aparecían en la ella asociando así la foto con la cuenta personal del etiquetado. Además, una vez identificado, su IA puede identificar al etiquetado en cualquier fotografía que aparezca con lo que puede asociar una cuenta con la imagen física de su titular. Las quejas de los usuarios, que no habían sido informados de la aparición de esta nueva aplicación y muchos menos habían prestado su consentimiento, obligaron a reconsiderar el etiquetado modificándolo de modo que solo se publica la foto si la persona etiquetada ha prestado previamente su consentimiento.

5. La ubicación

El uso de la ubicación es similar al de las cookies de localización. Permiten identificar la posición geográfica del usuario con la idea de mejorar su experiencia dándole información de actividades que pueden ser de su interés y que tienen lugar en su área geográfica. En su propia política de datos advierte "*usamos tu ubicación actual, el lugar donde vives y los lugares que te gusta visitar, así como las empresas y las personas que se encuentran cerca de ti, para proporcionar, personalizar y mejorar nuestros Productos, incluidos los anuncios, a fin de que resulten más pertinentes para ti y otras personas. Este tipo de información puede basarse en datos como la ubicación precisa del dispositivo (si nos has permitido recopilar esta información), direcciones IP e información de uso de los Productos de Meta (como registros de visitas y eventos a los que asistes".* Con el análisis de la ubicación FB puede establecer patrones de comportamiento, ya que utiliza hasta tres criterios de ubicación y además para conseguir esa localización además de usar el GPS del dispositivo (es lo que significa *"ubicación precisa")* puede usar las direcciones IP así como la información obtenida de otras aplicaciones. El rastreo de la ubicación puede ser desactivado por el usuario en el apartado "Configuración" de su cuenta en FB. Aunque esto no quiere decir que no pueda conocer dónde hemos estado porque recibe esa información a través de las cookies de aplicaciones con las que comparte información.

iii. Lo que sabe de nosotros

En realidad, deberíamos decir qué no sabe de nosotros. Con la información aportada por el propio usuario y la información obtenida por el algoritmo de comportamiento de Facebook probablemente lo sabe todo de nosotros. Hemos detallado en páginas anteriores qué datos aporta el propio usuario y cuáles conoce mediante su algoritmo, a partir de las interacciones y otras aplicaciones. Lo relevante para este trabajo es qué información obtiene una vez aplicado su algoritmo pero sobre esta cuestión no hay rastro alguno en su su política de datos. En cuanto al uso de los datos en sí nos encontramos con una respuesta genérica, ambigua y poco precisa, afirmando que "*utiliza nuestros datos para proporcionar, personalizar y mejorar (sus) productos*".

La clave de bóveda de la actividad de esta red social es su capacidad de microsegmentación y localizar nichos de mercados, lo que supone un ahorro enorme en costes a los anunciantes y unas tasas de efectividad altísimas que no les proporciona ningún otro medio publicitario. No hay que olvidar que tiene 2.900 millones de usuarios interactuando, generando millones de datos que son analizados y que de ese análisis detecta patrones y predisposiciones, que le sirven para prever el comportamiento de los usuarios a los que con un pequeño estímulo puede incitar a comprar un producto o votar a un partido político.

d. Su política de privacidad y condiciones del servicio.

Facebook ha lidiado desde sus orígenes con problemas relativos a la privacidad de sus usuarios. Cada innovación introducida ha provocado efectos indeseados en la privacidad de los usuarios generando críticas e investigaciones por parte de las autoridades. Así, p.e. en 2010 cuando incorporó a su aplicación el etiquetado fotográfico sin avisar ni pedir autorización a los usuarios, o cuando lanzó la aplicación "Open Graph" de gestión de metadatos y permitía el acceso a datos de usuarios de FB por parte de programadores de aplicaciones ajenos a la compañía y que fue el origen del escándalo de Cambridge Analytica.

Un alto cargo de FB manifestó que "La personalización no tiene que ser a expensas de la privacidad"[33] pero la realidad y la experiencia demuestran que la privacidad no ha sido

[33] Frase atribuida a Alex Stamos, ex Jefe de Seguridad de Facebook.

nunca una de sus prioridades. Nuestra privacidad es su negocio. Las condiciones del servicio recogen las normas por las que se rige el uso de FB.

e. El consentimiento del usuario

i. Administrar tu actividad

Esta aplicación permite al usuario clasificar sus publicaciones y actuar sobre ellas teniendo la posibilidad de decidir cuales quiere retirar para que no puedan ser vistas por el resto de los usuarios. También puede borrar definitivamente publicaciones.

ii. Verificación de privacidad

Permite seleccionar qué información personal se comparte, qué personas pueden ver las publicaciones y quién puede interactuar con el usuario. También permite revisar las formas en las que se puede localizar a otros usuarios y quien puede o no enviar solicitudes de amistad. En este apartado se encuentra la relación de otras aplicaciones con las que FB comparte información.

iii. Ver y descargar tu información

FB permite descargar toda la información que tiene sobre ti. En realidad, se trata sólo de la información que el usuario ha aportado desde la apertura de la cuenta y detalles de su actividad. La información está dividida en los siguientes bloques: perfil, información de contacto (dónde aparecen todos los teléfonos de tu agenda y direcciones de correo electrónico), biografía, fotos, videos, amigos, mensajes, toques, eventos seguridad (dónde se pueden comprobar las sesiones activas, desde qué dispositivo se ha realizado, hora de conexión, calidad de la señal, dirección I.P. y hasta cuál es la compañía telefónica que da el acceso a internet), anuncios y aplicaciones (con las que se han compartido datos personales). El apartado anuncios es muy interesante porque es uno de los factores de perfilado de FB. Aquí encontramos todos aquellos "Ads Topics" por los que en algún momento hemos mostrado interés.

Lamentablemente no se obtiene información relativa al perfilado que ha realizado FB sobre el usuario. Este es el fundamento de la actividad que hace esta red social. Su perfilado es su ventaja estratégica respecto a otros medios publicitarios ya que permite al anunciante

dirigirse específicamente a un segmento específico de mercado. Pero además, como el algoritmo conoce la predisposición del usuario respecto a un producto o servicio la tasa de éxito de esa publicidad es especialmente alta.

Este es uno de los problemas que tiene el derecho a la intimidad. Somos titulares de nuestros datos, la norma nos da derechos de disposición sobre ellos, sobre su uso, podemos modificarlos, borrarlos o trasladarlos pero no podemos saber el resultado que se ha obtenido de su análisis. Esta debería ser la entelequia de la protección de datos. El dato y resultado de su análisis son inseparables porque forman parte de una misma cosa. No se trata de conocer cómo FB llega a sus conclusiones, pues forma parte de su secreto industrial. Pero sí tenemos derecho a conocer las conclusiones a las que llega pero este derecho, como tal, no está recogido en la norma. Sin ese conocimiento, el consentimiento que se presta al tratamiento de nuestros datos está incompleto y a solventar esta cuestión es dónde deben dirigir sus esfuerzos los legisladores.

Se debe perseguir la "trasparencia algorítmica" como contrapartida al secreto comercial o industrial. Los algoritmos no son neutros. Están influenciados por las ideas, prejuicios y prioridades de quienes los crean, aunque estos traten de ser asépticos en su elaboración. No me interesa cómo lo hacen, me interesa el resultado de lo que hace.

f. Autorregulación de la plataforma

i. ¿Por qué estoy viendo esto?

En 2019 FB introdujo una nueva herramienta en la publicidad que aparecía en el "news feed" de sus usuarios para "mejorar la trasparencia y el control". Con esta herramienta el usuario puede conocer la razón por la que ve el anuncio. Estas razones pueden ser variadas, pero en realidad corresponden a una segmentación establecida por las necesidades del anunciante. Así p.e. una marca de ropa deportiva podría elegir la zona geográfica a que va destinada su publicidad, establecer un rango de edad, y sobre todo seleccionar aquellos usuarios que el algoritmo ha detectado que son deportivamente activos.

ii. La preferencia de anuncios.

Esta herramienta permite al usuario conocer qué anuncios ha visto o sobre los que haya hecho "click", y decidir si quiere seguir viéndolos o por el contrario quiere dejar de ver alguna categoría de anuncios (p.e. Viajes, hoteles, animales, etc) o anunciantes.

iii. Actividad fuera de Facebook

Este es un apartado importante al que me he referido anteriormente. Se trata de otra importante fuente de información para FB. Son los datos que otras aplicaciones y páginas webs comparten con FB. Muchas de esas aplicaciones y webs son gratuitas y su fuente de ingresos es la publicidad. La información que comparten (vía cookies) permite conocer si el usuario ha mostrado interés por algún tema en concreto lo que permite a FB mostrar contenidos y publicidad sobre ese tema.

g. El sesgo de percepción

i. Lo que nos gusta vs lo que creemos que nos gusta

Ya hemos visto que el algoritmo de Facebook está diseñado para conocer e interpretar nuestras preferencias y gustos. Esta decisión se basa en muchos ítems que valora en función de otros parámetros, la propia experiencia de uso y lo aprendido por la inteligencia artificial con otros usuarios con los que se comparten "elementos de conexión". Esto permite que FB incluya en el "news feed" del usuario publicaciones que considera optimas desde el punto de vista de las preferencias del cliente, pero, sobre todo, desde el punto de vista comercial. Esto no es más que la técnica del "*online behavioral advertising",* es decir la publicidad que vemos "solo" corresponde a nuestro comportamiento.

Pero en el "news feed" no aparece solo publicidad, también hay otro tipo de contenido esencial como son las publicaciones de otros usuarios con los que, sin ser conscientes el algoritmo ha detectado algún tipo de conexión (técnicamente correlación) o los "reels", una novedad introducida recientemente que son videos de corta duración. Estas publicaciones encajarían en "nuestras preferencias", de modo que casi todas ellas son de nuestro agrado.

La cuestión es si esa información que recibimos adultera nuestra percepción de la realidad. Es razonable plantearse que si solo vemos aquello que nos gusta o hace felices y nunca vemos nada que nos disguste, moleste o contrarie podamos acabar pensando que la

realidad es la que vemos y lo que no vemos no existe o simplemente es falso. Las redes sociales destacan por un uso brillante e interesado de los sesgos cognitivos de los usuarios creando un filtro burbuja que nos aleja de la realidad.

Un sesgo[34] es una distorsión de la información que recibe el individuo y que utiliza para la toma de decisiones o cómo se predispone ante circunstancias vitales o la valoración del riesgo.

ii. ¿Somos manipulados?

FB se ha convertido en una fuente de información para millones de personas, para muchos de ellos la única fuente. Pero la red social no es un medio de comunicación en sí, ya que no tiene línea editorial ni edita las publicaciones. Una red social no es más que una organización formada por grupos o individuos donde se relacionan unos con otros caracterizado por la existencia de flujos de información y dónde la única limitación para publicar la establecen las normas de uso estando totalmente prohibido la violencia o la incitación a la violencia, contenido violento o sexual. Fuera de esas limitaciones todo es posible aunque sea falso.

A principios de 2012 FB realizó un experimento con casi 690.000[35] de sus usuarios sin su conocimiento. El experimento en cuestión consistía en modificar la combinación del contenido que recibían en su "news feed". A una parte de los usuarios les mostró mayor cantidad de noticias positivas mientras que al otro grupo mostró más noticias negativas.

Los resultados del experimento dirigidos por investigadores de la Universidad de Cornell en California se publicaron en la revista "Proceedings of the National Academy of Science"[36]. Los resultados ponían de manifiesto que los usuarios que recibieron más noticias negativas tenían una mayor probabilidad de realizar publicaciones igualmente negativas. Y al contrario, quienes recibieron noticias positivas. De modo que se puede afirmar que Facebook puede manipular el estado emocional de sus usuarios.

---

[34] El concepto de sesgo cognitivo fue introducido en 1972 por los psicólogos israelíes Daniel Kahneman (Premio Nobel de Economía en 2002) y Amos Tversky en 1972.

[35] https://money.cnn.com/2014/06/30/technology/social/facebook-experiment/index.html?hpt=hp_t2 (Fecha de consulta 13/06/2022)

[36] Resultado de la investigación. https://www.pnas.org/doi/pdf/10.1073/pnas.1320040111 (Fecha de consulta 13/06/2022)

5. ¿CÓMO NOS PROTEGEMOS?

El desarrollo de la sociedad de la información y la tecnología es mucho más rápido que la capacidad de respuesta del legislador para resolver los problemas que esas innovaciones generan. Aunque sea consciente, la elaboración de una norma requiere de un análisis previo y una tramitación administrativo-parlamentaria que puede llevar años. Esos avances tecnológicos crean situaciones que son difíciles de prever. Y, por otra parte, la legislación debe ser compatible con el ejercicio de la libre empresa y debe facilitar el desarrollo, no impedirlo. Privacidad e innovación tecnológica no tienen por qué estar reñidos.

a. Normativa

i. Desarrollo normativo en los últimos años

No es hasta los años noventa del siglo pasado cuando realmente se inicia el despegue del desarrollo de la legislación específica a la protección de datos. El auge de los medios de pago electrónicos, "*el desarrollo de nuevas técnicas de recolección y almacenamiento de datos y acceso a los mismo ha expuesto a la privacidad a una amenaza potencial antes desconocida*"[37] y la necesidad de regulación del derecho a la protección de datos recogido en el art. 18.4 de la C.E., fueron los detonantes del inicio de este desarrollo normativo. Parece que ha llegado el momento de revisar los derechos fundamentales para obtener la versión 2.0. ya que probablemente estamos en una fase inicial de renovación, redefinición y ampliación de los derechos fundamentales como hasta ahora los hemos conocido.

ii. Normativa Europea

En cuanto a la normativa europea, los hitos normativos más relevantes en ese proceso han sido la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (derogada por el RGPD), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; la Directiva 97/66/CE del Parlamente Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones; el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y el Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos

[37] Exposición de motivos. L.O. 5/1992, de 29 de octubre, regulación dl tratamiento automatizado de los datos de carácter personal.

comunitarios y a la libre circulación de estos datos; la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y finalmente el Reglamento (UE) 2016/679 del Parlamento Europeo y el 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 RGPD. Esta norma de aplicación directa en toda la UE facilita a los ciudadanos que puedan ejercitar sus derechos y establece un marco común para todos los países. Entre sus novedades se encuentra; el establecimiento de la obligación de contar con consentimiento expreso del titular para el uso de datos. Se han ampliado, además, derechos incluyendo el derecho a la trasparencia (que "*exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y redactada en un leguaje sencillo y claro*"), el derecho de supresión, derecho de limitación y el derecho de portabilidad. Asimismo, establece la obligación de comunicar las brechas de seguridad a la Autoridad de Protección de Datos, entre otras novedades.

El desarrollo de esta normativa europea no ha sido fácil. Cualquier iniciativa se ha seguido muy de cerca por los EEUU y por los lobbies que gestionan las relaciones de las grandes ISP. Los encontronazos, las amenazas de sanciones, etc. han sido una constante cada vez que la UE intentado desarrollar una nueva norma. Así en 2016, las autoridades europeas y norteamericanas llegaron a un acuerdo, Decisión 2016/1250, por el que se regía la transferencia de datos entre Europa y los EEUU (punto siempre polémico), el "Privacy Shield". El acuerdo establecía condiciones que eran claramente favorables a las empresas americanas y que a efectos prácticos les permitía seguir transfiriendo datos sin limitación alguna. Este acuerdo sustituía a un acuerdo anterior del año 2000 de la Comisión Europea, Decisión 2000/520 "Safe Harbor"[38] que había sido declarado nulo por el Tribunal de Justicia de la Unión Europea [TJUE] en 2015 en base al acceso indiscriminado que los servicios de seguridad norteamericanos tenían a los datos de ciudadanos europeo, cuya información estaba alojaba en servidores situados en territorio estadounidense que es dónde tienen la sede la mayoría de las ISP. El acceso era indiscriminado y no proporcionado a los fines investigados.

[38] Decisión 2000/520 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (Fecha consulta 29-05-2022)

El "Privacy Shield" también fue declarado nulo por el TJUE[39] porque en su opinión este mecanismo no garantizaba una suficiente protección de los datos personales. El origen de esta disputa fue una denuncia presentada por un ciudadano austríaco llamado Maximilian Scherms contra Facebook Ireland, Ltd. por entender que la protección de datos que se deriva de la normativa interna de los EEUU relativa al acceso y la utilización por sus autoridades de los datos transferidos desde la UE no está regulada conforme a las exigencias equivalentes en el derecho de la UE. El Sr. Scherms (abogado de profesión) había solicitado a FB sus datos y comprobó que en ellos había violaciones de su intimidad y que además éstos se enviaban a EEUU. El problema no radicaba en la existencia de normativa interna sobre el acceso y utilización de datos personales por parte de las autoridades para fines de seguridad, sino en la falta de proporcionalidad de tal norma, que no limita los programas de vigilancia a lo estrictamente necesario.

Así las cosas y tras dos años de negociaciones, la UE y los EEUU[40] llegaron a un acuerdo el pasado 25 de marzo de 2022 por el que se establece un nuevo marco legal de las transferencias de datos personales entre ambos territorios denominado "Marco Transatlántico de Protección de Datos[41]". Este nuevo acuerdo según la UE "*facilitará una mayor cooperación entre y la UE, incluso a través del Consejo de Comercio y Tecnología y a través de foros multilaterales, como la Organización para la Cooperación y el Desarrollo Económicos, sobre políticas digitales*".

iii. Legislación Nacional

Los principales hitos en la legislación española relativa a la protección de datos son los siguientes: L.O. 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (derogada en 2000); L.O. 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (derogada parcialmente por LO 3/2018 de 5 de diciembre, varios artículos por RDL 5/2018); R.D. 1332/1994 de 20 de junio por el que se desarrolla determinados aspectos de la L.O. 5/1992 (derogado por RD 1720/2007) ; L.O. 15/1999, de 13 de diciembre de Protección de Datos y su Reglamento RD 1720/2007; Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio

[39] Sentencia Asunto C311/2018 Data Protection Commissioner Vs Maximilian Scherms, Facebook Ireland Ldt (Scherms II) https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9913101 (Fecha consulta 29-05-2022)

[40] Nota de Prensa del Acuerdo https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 (Fecha de consulta 29-05-2022)

[41] Texto completo del acuerdo. https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (Fecha de consulta 29-05-2022)

electrónico; L.O. 3/2018, de 5 de diciembre, de Protección de datos Personales y Garantía de Derechos Digitales; y finalmente la novísima L.O. 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que ha supuesto una mejora en respecto el intercambio de información entre cuerpos de seguridad, al establecer normas comunes, regula el tratamiento de datos genéticos y prohíbe la toma de decisiones basadas en mecanismos de tratamiento automatizado.

Además de estas normas el Ministerio de Asuntos Económicos y Transformación digital ha elaborado "La carta de derechos digitales[42]", que pretende recoger un conjunto de derechos necesarios para la protección digital del conjunto de la ciudadanía.

b. La nueva regulación europea que está por venir

i. Norma sobre Servicios digitales[43]

La norma sobre Servicios Digitales está destinada a usuarios, proveedores de servicios digitales y empresas usuarias de servicios digitales. Su objetivo es "crear un espacio digital más seguro y abierto para los usuarios, donde se protegen sus derechos fundamentales y les permite un acceso a servicios digitales de calidad a precios más bajos".

Esta nueva norma introduce mecanismos para la mejora de la defensa de los derechos de los ciudadanos estableciendo la obligación de información a los usuarios de la supresión de contenido y la posibilidad de oponerse a ello. Los usuarios tendrán acceso a mecanismos de resolución de litigios es su propio país. Se mejorará la trasparencia de las condiciones de uso de las plataformas. Se incrementará la seguridad y el conocimiento de los vendedores reales que operan online. Adicionalmente, se establecerán nuevas medidas de protección de menores, así como la prohibición expresa de publicidad a usuarios específicos de plataformas online cuando los destinatarios sean menores o se usen datos sensibles.

En cuanto a las empresas, establece obligaciones[44] para las plataformas online y motores de búsqueda respecto a los riesgos de desinformación, transparencia sobre las

[42] Texto Completo Carta Derechos Digitales. https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf (Fecha de consulta 10/06/2022)
[43] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_es (Fecha de consulta 29-05-2022)
[44] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-users_es

normas de moderación de contenidos, la obligación de realizar auditorías independientes de gestión de riesgos incluidos sus sistemas algorítmicos. La obligación de aportar información sobre la publicidad que reciben destinatarios específicos como quién patrocina el anuncio, cómo y porqué se dirige a ese destinatario específico y también la prohibición de determinados anuncios destinados a destinatarios específicos. También establece la obligación de información clara respecto a los motivos por los que se recomienda determinado contenido a los usuarios. Se contempla el derecho de los usuarios a no participar en las recomendaciones de contenido basadas en los perfiles elaborados por sistemas automatizados. Se permitirá un mejor acceso a datos para que las autoridades y los investigadores comprendan mejor la viralidad online y sus repercusiones con vistas a reducir los riesgos sociales. Y finalmente, la participación de las plataformas en códigos de buenas prácticas con el fin de atenuar los riesgos. Fue aprobada el pasado 23 de abril de 2022 y entrará en vigor en quince meses o el 1 de enero de 2024, si esta fecha es posterior.

ii. Norma sobre Mercados Digitales[45]

El futuro reglamento sobre mercados digitales tiene por objetivo "…igualar las condiciones para todas las empresas digitales, independientemente de su tamaño. Fijando reglas claras sobre lo que las grandes plataformas de internet pueden y no pueden hacer en la UE ". Se trata de impedir el comportamiento oligopolístico de las grandes empresas aumentando la capacidad de decisión de los usuarios, limitando la autopromoción de sus productos y exigiendo la interoperabilidad de las plataformas de mensajería.

Una de las cuestiones más reprochadas a las grandes plataformas de internet es que limitan la aparición de nuevos competidores (tal y como hemos indicado para FB) bien adquiriéndolos o bien limitando el posicionamiento de los productos que ofrecen en detrimento de los productos ofertados por otras empresas. Se limitará la autoclasificación más favorable de sus propios servicios y productos. Será posible la desinstalación de programas que vengan preinstalados en los dispositivos y se establecerá la obligación de la interoperabilidad entre plataformas de mensajería.

[45] https://www.europarl.europa.eu/news/es/headlines/society/20211209STO19124/la-ley-de-mercados-digitales-y-la-ley-de-servicios-digitales-explicadas (Fecha de consulta 29-05-2022)

iii. Norma sobre inteligencia artificial

La Comisión Europea presentó en abril de 2021 una nueva propuesta para establecer un marco regulatorio de la UE sobre inteligencia artificial[46] (IA). En su presentación la Comisión afirma que "se espera que las tecnologías IA aporten una amplia gama de beneficio económicos y sociales para un gran número de sectores". Continúa afirmando que "serán especialmente útiles para mejorar la predicción, para optimizar las operaciones y la asignación de recursos y para personalizar los servicios". La Comisión es consciente de que los sistemas de IA tienen importantes implicaciones para los derechos fundamentales poniendo en peligro derechos como la libertad de expresión, la protección de datos personales y la privacidad o el derecho a la no discriminación.

El proyecto de ley de IA es el primer intento de promulgar una regulación global de la IA, del mismo modo que supuso el RGPD. El marco legal propuesto se centra en la utilización específica de los sistemas de IA y los riesgos asociados. La Comisión propone establecer una definición tecnológicamente neutral de los sistemas de IA en la legislación de la UE y establecer una clasificación para los sistemas de IA con diferentes requisitos y obligaciones adaptados a un "enfoque basado en el riesgo". Se prohibirían algunos sistemas de IA que presentan riesgos "inaceptables". Se autorizaría una amplia gama de sistemas de IA de "alto riesgo", pero sujetos a una serie de requisitos y obligaciones para acceder al mercado de la UE. Aquellos sistemas de IA que presenten solo un "riesgo limitado" estarían sujetos a obligaciones de transparencia muy leves.

c. ¿Qué derechos tienen los ciudadanos?

La configuración de los datos como elemento del derecho a la intimidad y su concepción como bien personal supone para el ciudadano un derecho de disposición que entre sus potestades incluye excluir quien pueden hacer uso de ellos o ser excluido. Esto se ha plasmado en los derechos de acceso, rectificación, supresión, a la limitación del tratamiento, a la portabilidad y de oposición. Todos ellos recogidos en el capítulo II de la L.O. 3/2018 de 5 de diciembre de protección de Datos Personales y garantía de derechos digitales que incorpora y amplía el RGPD.

Su detalle e implicaciones son las siguientes[47]:

1. Derecho de acceso. Art. 13

[46] https://ec.europa.eu/commission/presscorner/detail/es/qanda_21_1683 (Fecha de consulta 12/06/2022)
[47] https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos (fecha consulta 30-05-2022)

Permite al usuario obtener una copia de tus datos personales que son objeto del tratamiento, conocer los fines del tratamiento, qué categorías de datos personales quiere que se traten. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales. Este último punto hace referencia a la posibilidad de que los datos personales del usuario sean tratados en otros países distintos al de residencia del usuario. Esto es de especial relevancia para FB ya que su centro de análisis se encuentra en EEUU.

Este derecho permite también conocer el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo. La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento. El derecho a presentar una reclamación ante una Autoridad de Control (en España la AEPD). Cuando los datos personales no se hayan obtenido directamente del usuario, cualquier información disponible sobre su origen (otros proveedores de datos como p.e.: RRSS, colegios profesionales, instituciones, entidades financieras o compañías proveedores de servicios). La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el usuario tiene derecho a ser informado de las garantías adecuadas en las que se realizan las transferencias de dichos datos.

2. Derecho de rectificación. Art. 14

El ejercicio de este derecho supone que podrás obtener la rectificación de tus datos personales que sean inexactos sin dilación indebida del responsable del tratamiento. O en el caso de que esos sean incompletos derecho a que se completen los datos personales, inclusive mediante una declaración adicional.

3. Derecho de supresión (más conocido como derecho al olvido). Art. 15

Se puede ejercitar este derecho cuando concurra alguna de las circunstancias siguientes: a) Si los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, b) Si el tratamiento de los datos personales se ha basado en el consentimiento presado a la persona responsable, y se retira el mismo, siempre

que el citado tratamiento no se base en otra causa que lo legitime, c) Si ha existido oposición al tratamiento de datos personales al ejercitar el derecho de oposición en las siguientes circunstancias:

- El tratamiento de la persona responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos.
- A que los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia.

a) Si tus datos personales han sido tratados ilícitamente

b) Si tus datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique a la persona responsable del tratamiento

c) Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).

4. Derecho de a la limitación del tratamiento. Art. 16

Este nuevo derecho consiste en la obtención de la limitación del tratamiento de los datos que realiza el responsable. Este derecho presenta dos vertientes: Cuando sea impugnada la exactitud de datos personales, durante un plazo que permita al responsable su verificación o cuando haya oposición al tratamiento de personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los del usuario.

5. Derecho a la portabilidad. Art. 17

La finalidad de este nuevo derecho es reforzar aún más el control de los datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, el usuario reciba sus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y puedas transmitirlos a otro responsable del tratamiento,

siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

6. Derecho de oposición. Art. 18

Este derecho supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

a) Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles: El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
b) Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada: Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines.

d. ¿Cómo ejercerlos?

El art. 13 del RGPD establece las obligaciones a las que está sujeto el "responsable del tratamiento de datos" de una entidad cuando los datos hayan sido obtenidos directamente del interesado; y el art. 14 recoge qué información de deberá facilitar al interesado cuando los datos no se hayan obtenido directamente de éste. Estas obligaciones suponen la necesidad de suministrar al usuario información relativa a la identidad y lo datos de contacto del responsable (de tratamiento de datos), los datos de contacto del delegado de protección de datos, entre otros.

El ejercicio de los derechos señalados en el apartado anterior se ejercitará ante el responsable de tratamiento de datos y se caracterizan[48] por ser gratuitos, salvo que las solicitudes sean infundadas o excesivas. Las solicitudes se responderán en el plazo de un mes, aunque dependiendo de su complejidad se puede prorrogar este plazo dos meses más. El responsable está obligado a informar sobre los medios para ejercer esos derechos; forma de contacto, dirección postal, números de teléfono, etc. Si el responsable no da curso a la

[48] AEPD. Ejerce tus derechos. https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una autoridad de control, en España la Agencia de Protección de Datos.

6. CONCLUSIONES

A la vista de todo lo expuesto anteriormente podemos afirmar que en cuanto a la protección de nuestro derecho a la intimidad respecto a la capacidad de predicción de los algoritmos y su posible influencia en nuestras decisiones es evidente que la regulación actual es insuficiente. No aparece recogido en ninguna norma, nacional o comunitaria que obligue al tenedor de datos, a quien los analiza en busca de información, a informar de hasta dónde puede llegar ese conocimiento obtenido. Es cierto, que se ha dotado al ciudadano de eficaces herramientas de control de sus datos, aunque en mi opinión esas herramientas no son suficientes. Como he señalado anteriormente la legislación tiene una concepción del dato (personal) como algo dado, estático. Sin embargo, lo relevante es que con esa ingente cantidad de información y la capacidad de análisis (y su previsible incremento en el futuro) coloca a esos "proveedores de servicios" en situación de condicionar las decisiones de los usuarios cercenando su autonomía personal.

En cuanto a las "decisiones individuales automatizadas" parece haberse impuesto el criterio mercantil, aunque el usuario tiene derecho a no ser objeto de decisiones automatizadas este derecho decae cuando ese análisis es necesario para la "*celebración o ejecución de un contrato en el usuario y el responsable*" o el usuario haya prestado ese consentimiento previamente, que es lo que ocurre cuando se solicita un préstamo a una entidad financiera. De ese modo este derecho queda invalidado por convertirse el análisis en una condición necesaria. Si el resultado de la solicitud fuera negativo, teóricamente, el responsable debe garantizar el derecho a usuario a obtener la intervención humana, que el usuario exponga su punto de vista e impugnar la decisión. Pero este derecho es desconocido por la gran mayoría de los usuarios. Una situación distinta se daría si la decisión negativa a la solicitud tuviera que hacerse obligatoriamente por escrito con justificación de las razones en las que se funda tal negativa. En ese documento, se debería incorporar información relativa a los derechos que le asisten al solicitante, así como la información de los mecanismos que tiene a su disposición para rebatir la decisión tomada por el sistema automatizado. De este modo, la impugnación del rechazo de la solicitud

estaría fundada en razones reales (las informadas por el responsable) y no hipotéticas (las obtenidas por el solicitante a consecuencia de un proceso de elucubración).

a. Un nuevo enfoque en la protección de la privacidad

i. Autorregulación de las plataformas

La autorregulación está basada principalmente en códigos de conducta cuya finalidad es el establecimiento de normas deontológicas para el ejercicio de una determinada actividad empresarial o profesional. También pueden contener recomendaciones sobre buenas prácticas y fórmulas de solución de conflictos establecidas por los propios operadores y usuarios. Las ventajas del sistema de autorregulación son varias. Por un lado, la flexibilidad (se pueden adaptar fácilmente), su especialización, favorecen el desarrollo de estándares, etc. Además puede suplir parcialmente el vacío legal respecto a una actividad.

En diciembre de 2007 la FTC estableció unos principios básicos de autorregulación[49] para los sistemas de publicidad conductual con el fin de garantizar la protección de datos y cuyos principios esenciales eran la trasparencia y control para y por el consumidor, seguridad razonable y conservación limitada en el tiempo de los datos, el consentimiento expreso para los cambios en los acuerdos preexistentes de privacidad y el consentimiento expreso o (en su caso, negativa) al uso de datos especialmente sensibles para la publicidad conductual.

La experiencia ha demostrado no ha funcionado o al menos no ha funcionado como se esperaba (no hay más que ver la escasa contundencia con la que FB ha actuado contra las "fake news" durante la campaña presidencial americana) o en cuestiones relativas a la privacidad de sus usuarios[50]. Y esto tiene que ver con dos cuestiones relacionadas: en primer lugar, las redes sociales más importantes son norteamericanas, y en segundo lugar, la cuestión ya tratada en páginas anteriores sobre la diferente concepción y protección que tiene Europa y los EEUU sobre el derecho a la intimidad. Desde el lado americano priman los intereses de las empresas y su visión "laissez faire" del mercado. No es admisible que la posible afectación de un derecho fundamental sea regulada por agentes privados.

---

[49] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (Fecha de consulta 13/06/2022)

[50] Un ejemplo de esto ocurrió en 2009 cuando FB fue demanda por siete usuarios acusándola de actividades ilegales comenzando por los cambios en la privacidad realizados por la plataforma. Para solventar este turbio asunto FB llegó a un acuerdo con la FTC en el que aceptó someterse a una auditoría independiente de privacidad durante los 20 años siguientes y sin embargo esto no evitó el escándalo de Cambridge Analytica en 2012.

Las RRSS cuentan con su propia normativa de autorregulación pero ésta no suele estar dirigida a la forma en la que gestionan, almacenan o analizan los datos sino al contenido que se puede compartir en dicha red. Y en todo caso, está destinada a protegerse a sí misma y a eludir responsabilidades respecto al comportamiento de sus usuarios.

El caso de FB su autorregulación respecto a los contenidos está recogida en las "normas comunitarias" y se dividen en las siguientes categorías:

La primera categoría "Conductas delictivas y Violencia" donde están prohibidos la violencia y su incitación. Las personas y organizaciones peligrosas. La organización de actos vandálicos y el fomento de actividades delictivas y el fraude y engaños. Una segunda xcategoría que denomina "Seguridad", que engloba la prohibición de la promoción o publicaciones del suicidio o autolesiones. La explotación sexual, abuso y desnudo de menores. La explotación sexual de adultos, el bullying y ciberacoso, la trata de personas e infracciones de la privacidad.

Otra categoría importante es la de "Contenido inaceptable". El algoritmo de FB es capaz de leer nuestras conversaciones por lo que es capaz de detectar actividades prohibidas y pueden suponer el bloqueo e incluso el cierre de la cuenta. Las actividades son las siguientes: el uso de lenguaje que incita al odio, contenido gráfico violento (el sistema permite informar que la publicación tiene carácter violento permitiendo su visionado a mayores de edad y previo consentimiento expreso del usuario). Desnudos y actividad sexual de adultos y la promoción de servicios sexuales.

La Ética de debería ir más allá de las normas y del RGPD. Las empresas cuyo modelo de negocio está basado el resultado obtenido por algoritmos y de ese resultado son capaces de conocer la personalidad y la predisposición de sus usuarios deben hacer un esfuerzo en trasparencia haciendo públicas las respuestas a preguntas como ¿qué información obtienen de sus algoritmos? o ¿cuáles son los límites éticos que guían su actividad?, explicando claramente cuáles son los límites que no van a sobrepasar.

ii. La autorregulación del usuario

Parece difícil e inapropiado descargar la responsabilidad en el usuario si este no cuenta con toda la información, que le permita tomar decisiones debidamente fundadas. Los ISP juegan a su favor con lo que se ha denominado "la fatiga de la privacidad". No es habitual ni razonable exigir a un usuario que lea las condiciones de uso y la política de privacidad

cuando estas tienen la extensión de un TFG. Lo que sí le es exigible al usuario es cierto grado de prudencia y diligencia.

iii. Propuestas de regulación

A continuación propongo una serie de medidas en materia de protección de datos que mejorarían, en mi opinión, la protección de datos de los ciudadanos. Las medidas son las siguientes:

1. Disociación

De todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Es razonable que el tratamiento de datos permita segmentar o categorizar a un usuario en un determinado grupo dependiendo de distintos criterios. Lo que en mi opinión supone una grave violación de la intimidad de los usuarios es que, con los datos (no identificativos) aportados por el propio usuario, sus interacciones y las técnicas de análisis de los operadores, un tercero sea capaz de identificarlo de forma individualizada. Pero no solo eso, es que la capacidad de análisis permite prever el comportamiento futuro del usuario con una fiabilidad que supera el 90%.

El avanzado estado de la tecnología permite esa plena identificación individualizada, y por tanto puede ser objeto de estímulos más o menos subliminales que induzcan un determinado comportamiento, ya sea una simple compra o un voto en unas elecciones.

2. Limitación de cesión

Debe limitarse la capacidad de cesión de datos de una empresa a otra, de modo que solo sea posible una trasmisión desde el receptor original a un tercero, y siempre con consentimiento del usuario. No debería ser válido el mero consentimiento que se presta cuando se aceptan las "Condiciones/Términos del servicio" y las "Política de Privacidad". Hemos visto que el caso de las "cookies" del diario El Mundo éste comparte datos con más de 140 empresas de todo el mundo.

3. Información a término

Con "información a término" me refiero a la información obtenida por el tenedor de datos una vez que ha procedido a su análisis, es decir, a la categorización y una vez determinada la probabilidad estimada de comportamiento que un usuario puede tener una

vez sometido a un estímulo, sea publicitario o de cualquier otra naturaleza. Es necesario que el usuario sea fehacientemente informado de que, con la información que aporta y la obtenida mediante el análisis de los datos, el tenedor puede prever su comportamiento futuro. También debe recibir información sobre qué tipo de estímulos, más allá de la mera publicidad, puede recibir para influir en su comportamiento u opinión.

4. Prescripción del uso de datos

El establecimiento de un régimen de prescripción de los datos recibidos por parte de los usuarios si estos dejan estar activos durante un periodo de tiempo. El RGPD en su considerando 39 señala que "*el responsable de tratamiento de datos ha de establecer plazos para su supresión"*. Parece razonable fijar plazos en función de la actividad y la duración de la relación del usuario con el tenedor de los datos y no dejar esa decisión al libre albedrío de las empresas.

5. Comunicación efectiva a afectados en caso de fuga de datos

Cada cierto tiempo conocemos a través de los medios de comunicación que alguna compañía ha sufrido un ataque informático con robo de información[51]. Por una cuestión de reputación y de imagen la mayoría de esos robos eran ocultados hasta la entrada en vigor del RGPD en mayo de 2018, ya que hasta ese momento no existía la obligación legal de comunicar las fugas (o robos) de datos de carácter personal. En los arts. 33 y 34 se establece la obligación de comunicar a la autoridad de control competente y al interesado la violación de la seguridad de los datos personales "*a más tardar en 72 horas después de que se haya tenido constancia de ella [violación de seguridad]*. El art. 34.1 dice "*Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida* ". Aquí la cuestión es ¿cuándo entraña un alto riesgo?, ¿lo decide la empresa o el órgano de control?.

La respuesta a la pregunta anterior se encuentra en el R.D. 43/2021[52], de 26 de enero por el que se desarrolla el RDL 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que recoge en su anexo la clasificación/taxonomía de los ciberincidentes así como su nivel de peligrosidad. Creo que la comunicación debe hacerse

[51] https://www.elindependiente.com/economia/2022/05/31/laboral-kutxa-reconoce-haber-sufrido-un-ciberataque-contra-su-servicio-de-correspondencia/ (Fecha de consulta 31/05/2022)
[52] Texto del RD 43/2021 https://www.boe.es/eli/es/rd/2021/01/26/43

en todos los casos, informando específicamente qué datos han sido afectados, así como el establecimiento de un régimen de indemnizaciones automático para el caso de que un uso ilegítimo de esos datos provoque perjuicios, de la naturaleza que sea a los usuarios.

6. Otra forma de gestión de la privacidad

El principio de trasparencia exige que "*toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro*". No se puede esperar de los usuarios una lectura completa de la política de privacidad y aunque sea leída es probable que no pueda comprender todos los términos sus consecuencias, aunque se utilice un lenguaje "*sencillo y claro*". Tampoco es posible una aceptación parcial ni negociar sus términos. Es un mero contrato de adhesión. Acabamos aceptando y luego, en caso de problemas, la empresa siempre puede alegar que hemos dado nuestro consentimiento. En consecuencia, el modo de protección de nuestra privacidad se basa en la suposición errónea de que contamos con toda la información. ¿Tenemos otra alternativa o damos por perdida la batalla de privacidad? Un lenguaje más simple seguramente incrementará la extensión de la política de privacidad, lo que no parece la alternativa más adecuada si lo que se busca es la simplificación. La opción razonable es que los "proveedores" recopilen menos datos, sólo los estrictamente necesarios para su servicio. En caso de querer más datos, que esto sea opcional y una decisión del propio usuario. Otra opción para simplificar el consentimiento es establecer una ficha estándar de datos, obligatoriamente descargable en el smartphone, ordenador o tablet, común para todos los proveedores y similar a la usada para los contratos de crédito por las entidades financieras[53], donde de forma simplificada y esquemática el usuario recibe una información comprensible de los elementos esenciales de la cesión de datos.

7. Ofuscación

A modo de protesta. Los profesores Finn Brunton, profesor de Medios, Cultura y Comunicación en la Universidad de Nueva York y Helen Nissenbaum[54], profesora de Ciencias de la información en la Universidad de Cornell (y una autoridad mundial en Privacidad) publicaron el libro titulado "Ofuscación" dónde abogan por el uso deliberado de información ambigua, confusa o engañosa que interfiera los procesos de recopilación de

[53] Ejemplo de documento INE Información Normalizada Europea para un crédito. http://app.bde.es/clf_www/leyes.jsp?id=102904&fc=07-12-2017&idart=102961&tipoEnt=0
[54] Página corporativa de la profesora Hellen Nissenbaum. https://tech.cornell.edu/people/helen-nissenbaum/ (Fecha de consulta 30/05/2022)

datos. Este planteamiento ha dado lugar a una tecnología[55] denominada de igual forma, que tiene por objeto enmascarar (no solo cifrar) la información almacenada en un sistema para protegerla de intrusiones externas.

8. Otras propuestas en relación con los ISP

a. Limitación de acceso a mercados adyacentes.

   Prohibición de nuevas adquisiciones de otras empresas.

b. Prohibición de la autopreferencia.
   La prohibición de la autopromoción de los productos y servicios del ISP en detrimento de los ajenos.

c. Fortalecimiento de las leyes de competencia.

   Parece necesario a la vista de lo sucedido en los últimos años una revisión de la normativa de competencia.

d. Revitalización de la aplicación del derecho antitrust.

   Hace años que no se han tomado por parte de los reguladores de la competencia europeos y norteamericanos, medidas contra alguna empresa obligándola a desprenderse de importantes unidades de negocio para acabar con su posición de monopolio. Este es un tema controvertido, sobre todo porque las empresas más importantes de internet son norteamericanas y las diferentes administraciones de ese país siempre se han mostrado muy beligerantes con la UE cuando ésta ha desarrollado una nueva legislación que les afectaba (p.e. la mal llamada "Tasa Google" o el mismo RGPD) amenazando incluso con la imposición de sanciones económicas. La nueva norma de "Mercados Digitales" avanza en este sentido.

Todas estas propuestas tienen por objetivo que el usuario tenga el pleno control de sus datos, del uso de sus datos, y un conocimiento del resultado del análisis de sus datos. Se trata pues de que tenga un conocimiento pleno de las consecuencias que la cesión de sus datos puede tener y, en caso de uso indebido o fraudulento, derecho a una indemnización automática sin necesidad de iniciar un costoso litigio judicial.

[55] https://www.ibm.com/docs/es/qradar-on-cloud?topic=protection-how-does-data-obfuscation-work (Fecha de consulta 31/05/2022)

7. BIBLIOGRAFÍA.

ÁLVAREZ CONDE, ENRIQUE Y TUR AUSINA, ROSARIO, Derecho Constitucional, Editorial Tecnos, Madrid, 2019.

BARTH, SUSANNE Y DE JONG, MENNO D. T. "*The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review"*. Elseviers. Telematics and Informatics, vol. 34, n.º 7, pp. 1038-1058, noviembre 2017. https://www.sciencedirect.com/science/article/abs/pii/S0736585317302022

BRUNTON, F Y NISSENBAUM, H, *Obfuscation: a user's guide for privacy and protest*, The MIT Press, Cambridge, 2015.

BYUNG-CHUL HAN, *Psicopolítica*, Editorial Herder, Barcelona, 2014.

CAMUÑEZ RUIZ, JOSÉ ANTONIO Y BASULTO SANTOS, JESÚS, *En el Alumbramiento de la Estadística Moderna: John Graunt*. Septem Ediciones, Oviedo, 2012.

CASAS BAAMONDE, MARÍA EMILIA (Coordinadora), El derecho a la protección de datos personales en la sociedad digital, Editorial Centro de Estudios Ramón Areces, Madrid, 2020.

FRENKEL, SHEERA Y KANG, CECILIA, Manipulados. La batalla de Facebook por la dominación mundial, Editorial Debate, Madrid, 2021.

FUSARO, DIEGO, Pensar diferente. Filosofía del disenso, Editorial Trotta, Madrid, 2022.

Guía de Protección de Datos y Garantía de Derechos Digitales: Nueva L.O. 6/2018 y Reglamento UE, Editorial Sepin, Madrid, 2018.

HARARI, YUVAL NOAH, Homo Deus. Breve historia del mañana, Editorial Debate, Madrid, 2016.

KREBS, BRIAN, "*Target Investigating Data Breach",* Krebs on security, diciembre de 2013. https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

LLANEZA, PALOMA, *Datanomics,* Editorial Deusto, Madrid, 2019.

LÓPEZ JIMÉNEZ, DAVID. *La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: El valor de la autorregulación*. Anuario Facultad de Derecho, Universidad de Alcalá, Madrid, 2009.

LÓPEZ ZAFRA, JOSÉ MANUEL Y QUERALT SÁNCHEZ DE LAS MATAS, RICARDO, Alquimia. *Cómo de los datos de están transformando en oro*, Editorial Deusto, Madrid, 2019.

MOLINER, MARÍA, *Diccionario del uso del español*. Segunda edición. Editorial Gredos, Madrid, 2006.

OLLERO, ANDRÉS, De la protección de la intimidad al poder de control sobre los datos personales, Real Academia de Ciencias Morales y Políticas, Madrid. 2018.

PRIETO GUTIÉRREZ, JOSÉ MARÍA, Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales, Boletín del Ministerio de Justicia, Madrid, 2004.
ROBSON, DAVID, La Trampa de la inteligencia. Por qué la gente inteligente hace tonterías y cómo evitarlo, Editorial Paidós, Barcelona, 2019.

SULLIVAN, CLARE, "Digital Identity: An Emergent Legal Concept The role and legal nature of digital identity in commercial transactions", University of Adelaide Press, 2011. Puede consultarse en http://www.jstor.org/stable/10.20851/j.ctt1sq5wqb.1.
TOMÁS DE LA CUADRA SALCEDO – JOSÉ LUIS PIÑAR Mañas (Directores), Sociedad Digital y Derecho, Boletín Oficial del Estado, Madrid, 2018.

VARIOS AUTORES. *Usos militares de la inteligencia artificial, la automatización y la robótica* (IAA&R). Ministerio de Defensa. Secretaría General Técnica, Madrid, 2020.

ANEXO NORMATIVO.

Constitución Española de 1978.

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.

Ley Orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal.

Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.

Ley Orgánica 3/2018, de 2 de diciembre de protección de datos personales y garantía de derechos digitales.

RD. 1720/2007, de 21 de diciembre Reglamento de desarrollo de la L.O. 15/1999 de protección de datos de carácter personal.

RDL 5/2018, de 27 de julio de medidas urgentes para la adaptación del derecho español a la normativa de la UE en materia de protección de datos. (Derogado)

RD 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)

DIRECTIVA (UE) 2018/1972 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas

REGLAMENTO (UE) 2019/1150 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea

PÁGINAS WEB

[1]www.aepd.es

[2] www.sama.com

[3]https://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

[4]https://elpais.com/ideas/2022-05-09/joanna-pocock-las-redes-provocan-una-separacion-entre-cuerpo-y-realidad.html?utm_source=pocket_mylist

[5]https://elpais.com/cultura/2022-05-04/eric-sadin-nos-gusta-la-idea-de-ser-monitorizados.html?utm_source=pocket_mylist

[6]https://elpais.com/tecnologia/2022-05-05/xinjiang-es-el-primer-gran-modelo-en-la-era-de-la-vigilancia-digital-masiva-nunca-se-ha-visto-nada-igual.html?utm_source=pocket_mylist

[7]https://www.xataka.com/legislacion-y-derechos/ley-servicios-digitales-dsa-obligara-a-big-tech-a-explicar-sus-algoritmos-cede-demasiado-poder-camino?utm_source=pocket_mylist

[8]https://www.lawandtrends.com/noticias/despachos/llego-la-hora-de-tomar-las-riendas-de-tu-identidad-digital-1.html?utm_source=pocket_mylist

[9]https://elpais.com/opinion/2022-04-19/la-etica-del-algoritmo.html?utm_source=pocket_mylist

[10]https://elpais.com/ideas/2021-04-17/grandes-datos-pequena-politica.html?utm_source=pocket_mylist

[11]https://www.elmundo.es/economia/actualidad-economica/2022/03/25/6231ece7fc6c8338778b45c6.html?utm_source=pocket_mylist

[12]https://cms.law/es/esp/publication/la-publicidad-del-dato-personal-no-otorga-per-se-legitimacion-para-su-tratamiento?utm_source=pocket_mylist

[13]https://www.elconfidencial.com/cultura/2022-03-07/niklas-maak_3385911/?utm_source=pocket_mylist

[14]https://elpais.com/opinion/2022-02-10/las-amenazas-de-facebook.html?utm_source=pocket_mylist

[15]https://www.abc.es/antropia/abci-discriminacion-analisis-datos-20220124141437_noticia.html?utm_source=pocket_mylist

[16] https://elpais.com/tecnologia/2022-05-24/me-preocupa-que-las-grandes-companias-como-google-microsoft-facebook-o-amazon-tengan-recursos-casi-infinitos.html?utm_source=pocket_mylist

[17] https://elpais.com/tecnologia/2022-05-17/google-revisa-la-localizacion-y-actividad-online-de-los-espanoles-426-veces-al-dia.html?utm_source=pocket_mylist

[18] https://www.technologyreview.es//s/11980/los-cinco-mejores-libros-sobre-la-importancia-de-predecir-el-futuro?utm_source=pocket_mylist

[19] https://elpais.com/economia/negocios/2022-05-18/quien-controle-los-datos-dominara-el-mundo-y-espana-tiene-una-posicion-privilegiada.html?utm_source=pocket_mylist

[20]https://www.elmundo.es/tecnologia/2022/04/27/62690ef421efa0ec4d8b45e8.html?utm_source=pocket_mylist

[21] https://www.xataka.com/legislacion-y-derechos/ley-servicios-digitales-dsa-obligara-a-big-tech-a-explicar-sus-algoritmos-cede-demasiado-poder-camino?utm_source=pocket_mylist

[22] https://www.technologyreview.es//s/11980/los-cinco-mejores-libros-sobre-la-importancia-de-predecir-el-futuro?utm_source=pocket_mylist

[23]https://bandaancha.eu/articulos/europa-regulara-seguridad-routers-10234?utm_source=pocket_mylist

[24]https://elpais.com/opinion/2022-04-19/la-etica-del-algoritmo.html?utm_source=pocket_mylist

[25] https://www.elespanol.com/omicrono/software/20210403/datos-millones-usuarios-facebook-espana-filtrados/570943394_0.html?utm_source=pocket_mylist

[26]https://www.elmundo.es/papel/futuro/2020/05/05/5eab58e621efa05c288b45d5.html?utm_source=pocket_mylist

[27]https://www.elmundo.es/economia/actualidad-economica/2022/03/25/6231ece7fc6c8338778b45c6.html?utm_source=pocket_mylist

[28]https://www.abc.es/ciencia/abci-markus-gabriel-nuevo-facebook-heroina-mental-habria-prohibirlo-202111070114_noticia.html?utm_source=pocket_mylist

[29] WhatsApp es bastante intrusivo y Facebook es un "buitre de los datos": Carissa Véliz, experta en privacidad y protección de información. https://www.bbc.com/mundo/noticias-55683865?utm_source=pocket_mylist

[30] https://www.cpomagazine.com/

[31] https://edps.europa.eu/_en

[32] https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

[33] Cuena, Matilde. https://indret.com/intercambio-de-informacion-positiva-de-solvencia-y-funcionamiento-del-mercado-de-credito/

[34]https://www.ft.com/content/c93725c4-5e34-4b3b-aae8-dd4c241abebd?utm_source=pocket_mylist

[35] https://www.youtube.com/watch?v=aA_VFXDcVvw

[36] https://edpb.europa.eu/edpb_es

[37] https://thenai.org/

[38] https://www.tribunalconstitucional.es/es/Paginas/default.aspx

[39] https://guiasjuridicas.wolterskluwer.es/