

Disociados (Desdoblados). El futuro social de la humanidad

Francisco Marco Fernández



Reial Acadèmia Europea de Doctors
Real Academia Europea de Doctores
Royal European Academy of Doctors

BARCELONA - 1914



FRANCISCO MARCO FERNÁNDEZ (Barcelona 1972).

Doctor en Derecho por la Universitat Autònoma de Barcelona (2002) con la calificación de Sobresaliente “*Cum Laude*” por la tesis doctoral “La investigación privada y el derecho a la *privacy*”.

Precursor de trabajos sobre la problemática en Internet y el derecho a la *privacy* realizó ya en 1998 un trabajo doctrinal sobre la materia (“La protección de los datos personales automatizados en las redes mundiales de la información”) y le fue concedido el tercer Premio Nacional de Doctrina en el año 2000 por el trabajo doctrinal: “La monitorización del correo electrónico en la empresa”.

Licenciado en Derecho por la Universidad de Barcelona (1995), obtuvo además el grado de investigación privada en la Universidad de Barcelona (1994) y es máster en derecho de sociedades del Colegio de Abogados de Barcelona (1996). Autor de numerosos escritos doctrinales sobre el derecho a la *privacy* y sobre la inteligencia de datos y la profesión de investigación privada.

Desde los 25 años dirige uno de los mayores grupos de inteligencia empresarial español. Impulsor de la inclusión de la figura del investigador en la Ley de Enjuiciamiento Civil es miembro de la *Association of Certified Fraud Examiners*.

Autor de doce libros de divulgación, tres de ellos han sido número uno de ventas en nuestro país.

**Disociados
(Desdoblados).
El futuro social
de la humanidad**

Excmo. Sr. Dr. Francisco Marco Fernández

Disociados (Desdoblados). El futuro social de la humanidad

Discurso de ingreso en la Real Academia Europea de Doctores, como
Académico Correspondiente, en el acto de su recepción
el 7 de junio de 2022

por

Excmo. Sr. Dr. Francisco Marco Fernández
Doctor en Derecho

y contestación del Académico Numerario

Excmo. Sr. Dr. Fermín Morales Prats
Doctor en Derecho

COLECCIÓN REAL ACADEMIA EUROPEA DE DOCTORES



Reial Acadèmia Europea de Doctors
Real Academia Europea de Doctores
Royal European Academy of Doctors
BARCELONA · 1914

www.raed.academy

© Francisco Marco Fernández
© Real Academia Europea de Doctores

La Real Academia Europea de Doctores, respetando como criterio de autor las opiniones expuestas en sus publicaciones, no se hace ni responsable ni solidaria.

Quedan rigurosamente prohibidas, sin la autorización escrita de los titulares del “Copyright”, bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático y la distribución de ejemplares de ella mediante alquiler o préstamos públicos.

Producción Gráfica: Ediciones Gráficas Rey, S.L.

Impreso en papel offset blanco Superior por la Real Academia Europea de Doctores.

ISBN: 978-84-09-41712-4

D.L: B-11975-2022

Impreso en España –Printed in Spain- Barcelona

Fecha de publicación: junio 2022

ÍNDICE

PRESENTACIÓN	9
DISCURSO DE INGRESO	11
CAPÍTULO 1. EL TOTALITARISMO DE LA ATENCIÓN	11
<i>Engagement</i> : las trampas de los algoritmos	12
Nos observan.....	14
El camino hacia este futuro: “ <i>Google is the competitor</i> ”.....	17
El poder de las corporaciones	22
La magia china	25
CAPÍTULO 2. HACIA LA SOCIEDAD HIPERINDIVIDUALISTA ...	29
Hacia la nueva esclavitud y la transformación social	31
La doble personalidad jurídica: identidad 2.0	34
El derecho de los datos	37
CAPÍTULO 3. HACIA UN NUEVO CONTROL SOCIAL EN LA ERA DIGITAL.....	39
Hacia un contrato social digital	40
El nuevo humanismo.....	43
El no contrato social en China	44
El contrato social individualista de los norteamericanos.....	47
El padre Estado europeo.....	50
Hacia un contrato social digital humanista basado en la confianza.....	52
El nuevo contrato social de la humanidad.....	54
CAPÍTULO 4. EL POPULISMO ROBÓTICO, LA EDUCACIÓN Y EL <i>BIG DATA</i>	59
El miedo a las máquinas: máquinas vs humanos	61
Personalidad jurídica de los robots.....	65
La cadena de valor: el hombre en la quinta revolución industrial	68
La quinta revolución industrial.....	71
CAPÍTULO 5. EL FUTURO	77
Los datos generan temor y populismos	80
El futuro está en la cesión de los datos de carácter personal.....	81
Internet la nueva tierra de los comunes.....	83
Los nuevos peligros y la justicia privada.....	89

CAPÍTULO 6. LOS DERECHOS EN LA QUINTA REVOLUCIÓN INDUSTRIAL Y LOS TECNOAGOREROS.....	93
La hiperprivacidad un problema del siglo XXI.....	99
Seguridad y el sesgo algorítmico	101
CAPÍTULO 7. LOS NUEVOS HEREJES: LOS DATOS	107
La exigencia de privacidad en la era de la individualidad.....	111
La paradoja de Pulgarcito	113
La paradoja de la incongruencia digital.....	116
El data driven: los datos en el centro de la empresa.....	119
El internet de las cosas (IDC): la integridad y seguridad es más importante que la privacidad	122
El caso Carpenter: el cambio de paradigma internacional	123
Hacia la protección del entorno digital y no de la persona analógica.....	128
CAPÍTULO 8. ¿HEMOS ACEPTADO SER ESPIADOS?.....	133
La teoría de la “integridad contextual”	138
Nuestra morada informática.....	141
El efecto spillover en los datos	143
La identidad digital	145
CAPÍTULO 9. PROTEGER NUESTROS DATOS: HACIA LA TRANSPARENCIA.....	149
El derecho a la intimidad en la era de internet: la privacidad	150
Hacia una gestión de la confianza y no de la intimidad.....	152
El sesgo del desdoblamiento	156
El sesgo del alma y la caja de la privacidad: la solución real.....	160
La paradoja de la privacidad	162
La exigencia de transparencia.....	164
CAPÍTULO 10. HABLEMOS DE DINERO: UNA RENTA BÁSICA POR NACER.....	167
Derecho sobre los datos.....	168
Renta básica	171
El doble contrato social	172
Sistema de gestión de tráfico de datos.....	175
CONCLUSIONES	179
DISCURSO DE CONTESTACIÓN.....	181
Publicaciones de la Real Academia Europea de Doctores	199



❖ PRESENTACIÓN

Excmo. Sr. Presidente de la Real Academia Europea de Doctores, Dr. Alfredo Rocafort Nicolau

Excmos. Sres. Académicos

Señoras y Señores,

Es para mí un honor poder estar aquí hoy delante de ustedes dispuesto a dar lectura al Discurso preceptivo de Recepción como Académico Correspondiente en esta Real Academia Europea de Doctores.

Pero este honor lo debo. Lo debo fundamentalmente a los tres académicos que me han propuesto, los Dres. Fermín Morales, Xabier Añoveros y Joan Francesc Pont, así como a esta Real Academia por su confianza y benevolencia en aceptar la propuesta. Espero ser merecedor de ello.

Lo debo también, a mi familia, que siempre me apoya y me perdona las muchas horas que le sustraigo de dedicación a hobbies y a otros menesteres.

Lo debo a mis maestros que me acompañan desde los inicios de mi formación, especialmente a los profesores Fermín Morales y Cristóbal Martell.



❖ CAPÍTULO 1. EL TOTALITARISMO DE LA ATENCIÓN

Las imágenes han desplazado a las palabras. Los creadores de internet han conseguido que unas pocas empresas tengan más poder y más dinero que muchos estados simplemente “enganchándonos” a la sencillez de lo visual y a la ilusoria gratuidad. Han conseguido mantenernos frente a la pantalla con trampas psicológicas que permiten controlar nuestros movimientos digitales y ha provocado que nuestra personalidad se disocie.

La comunicación digital y la vida a través de una pantalla nos ha convertido en seres individualistas. Buscamos sentirnos diferentes y especiales, no ya a través de la propiedad sino de la imagen. Hemos entrado en un proceso de individualización en el que el mundo se centra en uno mismo. Hemos sustituido a la familia y el ágora (el salón familiar) por la habitación, la puerta cerrada y el teléfono móvil como ventana hacia los demás. Esto significa que la soledad es una nueva forma de convivencia. Y en cuanto nos apartamos de la masa aparece lo íntimo, lo privado y el individualismo: el derecho a la intimidad. Nos hemos convertido, de golpe, en una suerte de hombre primitivo encerrado en casa por devoción que se comunica digitalmente. Somos, cada día más, digitales socialmente e individualistas analógicamente. Protegemos la privacidad en nuestra morada y la regalamos en Internet.

Es cierto, el futuro ha llegado y ha desdoblado nuestra personalidad jurídica. El nacimiento determina la personalidad y la muerte la extingue; sin embargo, con la amortización de la cuarta revolución industrial, y la quinta a punto de llegar, se atisba la

existencia de una doble personalidad en todos los individuos, una analógica y otra digital. Ambas personas, la digital y la analógica, son diferentes lo que ha provocado -y provocará más aún- una dicotomía jurídica, económica, social y psicológica en un mismo individuo. Como se comprobará en este trabajo, esa personalidad digital (identidad digital) no solo se configura con lo que decimos de nosotros mismos, sino que se complementa con lo que los demás pueden recopilar de las pistas (migajas de pan) que vamos dejando mientras navegamos. Es lo que se conoce como la paradoja de Pulgarcito. Navegamos y dejamos ir pistas de nuestra identidad digital que alguien agrega y estudia. Y esa identidad digital es cada día más importante.

Pasamos 6 horas y 54 minutos al día navegando en la red de redes¹. La transformación digital ha provocado que los individuos pasemos un cuarto del día utilizando nuestra personalidad digital. Vivimos casi más tiempo navegando por internet, leyendo online, viendo series en *streaming* o realizando *zooms* que charlando en persona y necesitamos regular esta situación. Si no lo hacemos pronto seremos meras herramientas de cinco grandes corporaciones que controlarán nuestros datos, nuestra vida digital. Más si consideramos que son esas corporaciones las que provocan ese desdoblamiento digital con actividades sobradamente conocidas por la magia, pero ahora, en forma de algoritmo.

Engagement: las trampas de los algoritmos

Los magos e ilusionistas utilizan trampas psicológicas para lograr sus trucos. Mientras reímos cambian una carta o dirigen nuestra mirada hacia un punto para que en el contrario se produzca la ilusión. Engañan a nuestro cerebro capturando nuestra

¹ Recuperado en Digital Report 2021: El informe sobre las tendencias digitales, redes sociales y mobile.
- We Are Social ES

atención. Pues bien, las empresas tecnológicas hacen lo mismo. Epic Games es una de las mayores empresas de videojuegos del mundo y los creadores del famoso juego Fortnite que tantos titulares ha generado por la adicción que provoca -comparada con la cocaína- en nuestros hijos. Y es que los creadores de contenido digital nos necesitan pegados a la pantalla el mayor tiempo posible. El neurólogo Ramsay Brown señala que estamos frente a una “carrera armamentística para mantenernos frente a las pantallas”² donde pueden controlar nuestro alter ego digital, nuestra personalidad digital.

Es la época del totalitarismo de la atención. Nos quieren solos frente a la pantalla para ellos solos. Y nosotros creemos que socializar es eso. ¿Por qué si escuchamos música encima de una cinta de gimnasio caminamos más tiempo? Es sencillo: distraemos el cerebro del cansancio. Algo parecido pasa con el calor o el frío. Y eso lo saben los programadores. Nos piden datos mientras nos distraen con contenidos, música o una promesa de diversión. Entonces damos el clic, aceptamos su política de datos y ¡zas! ya somos suyos. Son dueños de parte de nuestra personalidad digital. Lo peor es que lo sabemos y no dejamos de hacer clic algo que, como veremos, se conoce como la paradoja de la privacidad. Datos a cambio de azúcar para el cerebro.

La dopamina es un neurotransmisor que trasmite a nuestro cerebro el químico del placer. Algunos científicos hablan de un secuestro de nuestra mente³ y advierten que en una econo-

² Citado en Peirano, M. El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención, Debate, 2019, p.78. Sobre la economía de la atención véase también Byung-Chun Han: La expulsión de lo distinto. Ed Herder (2017). Barcelona, ABC. Byung-Chul Han: «Hoy no se tortura, sino que se «postea» y se «tuitea»», The Guardian. 'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia, The Economist. The world's most valuable resource is no longer oil, but data.

³ 'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia. <https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia>

mía basada en la captura de la atención de los usuarios (antes llamados consumidores) para controlar nuestros gustos que se transforman “en datos que pueden ser vendidos o que pueden ser usados para hacer más inteligentes a las plataformas y generar anuncios más efectivos”⁴ nos llevará a ser esclavos de esas empresas.

Tocamos la pantalla 2617 veces al día⁵; y cada vez que lo hacemos es como meter una moneda en una máquina tragaperras, como encender un cigarro o comer una chuchería. Hemos caído en la vieja trampa de los ilusionistas. Hacemos lo que quieren los programadores a cambio de un poco de dopamina. Y como con todas las sustancias adictivas debe regularse. Porque los datos se han convertido en el nuevo petróleo, quien los controle dominará el mundo, quien tenga datos que vender será rico y quien no tenga devendrá un homeless tecnológico, económico y social. Qué no decir de los poderes públicos que, al saberlo, regulan nuestra vida digital para poder controlar nuestro pasado analógico⁶. Y todo se hace observando nuestra rutina digital para que nuestra personalidad analógica compre un producto.

Nos observan

Somos lo que googleamos, es la verdad. La respuesta también la encontramos en la química. Aceptamos la política de privacidad igual que si comemos una patata frita y ya no podemos

⁴ Martínez Gallardo, A. *¿Qué es la dopamina digital y cómo se convirtió en la droga más popular y adictiva del mundo?* Altercultura. 2017 recuperado en *¿Qué es la dopamina digital y cómo se convirtió en la droga más popular y adictiva del mundo?* (pijamasurf.com)

⁵ <https://blog.dscout.com/mobile-touches>

⁶ Sobre el control informático de la libertad, el almacenamiento y la retención de datos vid. Morales García, O., *El control informático de la libertad (o la crónica de una muerte anunciada)*, en VVAA, Ruiz Rodríguez, L, *Respuestas Internacionales a los retos de la seguridad*, pp. 215-228, Tirant Lo Blanc, 2009.

parar de comer. La dopamina, como se ha señalado, tiene la respuesta y el contrato social la explicación. Necesitamos sentirnos aceptados y en la nueva era, las aplicaciones son las nuevas chucherías. Condicionan nuestra vida analógica para que pasemos más tiempo digitalizados y cediendo nuestros datos, nuestra privacidad, sin pensar que es el nuevo petróleo. La culpa la tiene el sesgo de deseabilidad social: mentimos para que el resto del mundo piense bien de nosotros, pero Google conoce nuestras mentiras, como los antiguos comités vecinales sabían lo que ocurría en nuestras casas.

La gente cuenta al buscador lo que no cuenta a nadie y Facebook analiza esos datos y ya nos ha capturado⁷. Y nosotros seguimos navegando o leyendo información, supuestamente real y gratuita, igual que las aplicaciones nos quieren gastando. Ese es el juego. Y como antaño las tabaqueras con la adicción a la nicotina lo ocultan. Han convertido a una nueva generación de niños en adictos a las pantallas para conseguir sus datos y enriquecerse con ellos⁸. Y esos niños no asumen que sus rastros quedan registrados y que los Gobiernos intentan controlarlos. Como acertadamente me hizo ver el profesor Óscar Morales García la tendencia legislativa actual persigue el control ciudadano, ya que sabe que, como señala la jurisprudencia del TJUE, “estos datos, considerados en su conjunto, pueden proporcionar indicaciones muy precisas sobre la vida privada de las personas cuyos datos se conservan, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u

⁷ Davidowitz, S. *Todo el mundo miente: Lo que Internet y el Big Data pueden decirnos sobre nosotros*, Capitan Swing, 2019, p.12 y ss.

⁸ El año 2019 un bufete de abogados canadiense demandó a Epic Games, creadora del juego Fornite, acusándola de provocar la adicción al videojuego, comparando a la que sufren los adictos a la cocaína por la liberación de dopamina. La demanda asegura que las mecánicas de juego están especialmente diseñadas para fomentar la dependencia, para así enganchar a los jugadores.

otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados”⁹.

Todavía no se ha iniciado la gran batalla judicial, pero llegarán las grandes demandas y las advertencias como en las cajetillas de tabaco. “Navegar genera adicción y condiciona nuestra privacidad”. En 2013 un hombre de Nashville presentó una demanda contra la compañía Apple por vender computadoras con libre acceso a contenidos sexuales, lo que le convirtió en un “adicto a la pornografía”. En su demanda aseguró que “la pornografía había arruinado su matrimonio y envenenado su vida”; señaló que todo había comenzado después de que el navegador de Apple, Safari, en vez de dirigirle la página de Facebook le llevara a la página de pornografía Fuckbook¹⁰. La demanda no prosperó, pero finalmente cuando alguien encuentre las pruebas de cómo condicionan nuestra forma de relacionarlos lo hará.

Las demandas contra las empresas tabaqueras se fundamentaron en un *prius*: ‘*me enganchas con nicotina a sabiendas de que me mata*’. Hoy, el mensaje sería ‘*me enganchas con aplicaciones para conseguir mis datos y hacer negocio con ellos*’. Y ya hay voces que indican que empresas de software, como la citada Epic Games y su videojuego Fortnite, contrataron a psiquiatras para diseñar juegos que generen adicción en nuestros hijos. Los generadores de contenidos digitales son los nuevos dictadores.

⁹ La Directiva de la UE de retención de datos 2006 (Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas) actuó como respuesta a los problemas de seguridad detectados tras los atentados terroristas del 11-M en Madrid en 2004 y del 7-J en Londres en 2005 y obligaba a los proveedores a conservar los datos de tráfico y de localización, así como aquellos necesarios para identificar al abonado o al usuario. En cambio, no autorizaba la conservación del contenido de la comunicación ni de la información consultada. El Tribunal de Justicia de la Unión Europea dictó una sentencia en los asuntos acumulados C-293/12 y C-594/12, por la que anulaba la Directiva, por considerar que constituye “una injerencia de gran magnitud y especial gravedad” en los derechos fundamentales a la privacidad y a la protección de datos”.

¹⁰ Recuperado en https://www.bbc.com/mundo/ultimas_noticias/2013/07/130715_ultnot_eeuu_demanda_apple_pornografia_jg

Parece que nos digan: ‘*dame tu vida a cambio de un plato de comida gratis*’. Y es literal: nos dan diversión a cambio de nuestra vida digital. Usan nuestras emociones para convertirnos en fieles seguidores del gurú del algoritmo del *engagement*. Si vemos vídeos políticos Twitter nos ofrecerá ‘vídeos similares en el que nos inocularán el pensamiento político del que más pague’. Parece nuestro ayudante, nuestro amigo, pero no lo es. ‘*He encontrado esto para ti*’, nos dice. Y son sus algoritmos quienes se convierten en *nuestro* periodista de cabecera, en el operador que nos permite no pensar y seguir su mensaje a pies juntillas. Los algoritmos son los nuevos Mesías, los nuevos gurús. Nosotros sus cobayas. Y nuestra información el petróleo que mueve el mundo. Damos nuestros datos a cambio de dopamina sin ningún tipo de regulación y de protección del ciudadano. ¿Es el momento de un nuevo contrato social que nos proteja? O, por el contrario, ¿debemos ceder esa parte de nuestra personalidad a cambio de poder navegar y ser digitales? Para contestar a esas preguntas debemos conocer el origen del desdoblamiento de nuestra personalidad.

El camino hacia este futuro: “*Google is the competitor*”

Todo empezó en 2007.

El camino hacia este futuro se inició el día que Steve Jobs sacó del bolsillo de sus pantalones tejanos el primer Iphone, en el Moscone Center de San Francisco. El visionario fundador de la compañía de la manzana no sabía que aquel artefacto rectangular iba a provocar la revolución industrial más importante que ha sufrido la humanidad y, mucho menos, que con aquella histórica jornada se había puesto la primera piedra para la construcción de una nueva sociedad vigilada. Aquel 29 de junio de 2007 comenzó la digitalización de nuestra vida, la globalización del planeta y la construcción del arma más poderosa con

la que se puede llegar a perder nuestra libertad: el control social. Pero el exceso de información con el que vivimos no nos deja ver que el futuro está aquí y nos está absorbiendo.

Aquel primer iPhone era un dispositivo con pantalla táctil, conexión a Internet y cámara de fotos. La clave de su éxito fue la combinación de todos los elementos en un aparato muy sencillo de utilizar. En ese mismo año Twitter y Facebook despegaban. Google lanzaba Android, Amazon el lector Kindle e Internet dejaba de ser un reducto para convertirse en un todo¹¹. Aquel 2007 el coste de la secuenciación del ADN por persona pasaba de 100 millones de dólares a 1000 dólares¹². Hace pocas semanas he secuenciado el mío por 250 dólares y sé que comparto mis raíces antropológicas con españoles en un 75%, con búlgaros en un 10%, en un 8% con italianos y un 2% con marroquíes a pesar de que mi tez cetrina me hubiese hecho pensar que por mi sangre corría más sangre sefardita de la que tengo. También sé que tengo menos predisposición genética a tener cáncer de próstata y mayor a la enfermedad de Párkinson. Y todo lo hice poniendo una muestra de saliva en un bastoncillo; posteriormente, mis datos médicos viajaron por el ciberespacio y están almacenados en mi ordenador y en el de la empresa 24genetics. Todo esto comenzó aquel 2007 y hoy nuestra vida ha dejado de ser como los grandes filósofos pronosticaron.

Las magnitudes económicas no engañan. Facebook cuenta con más de 2200 millones de usuarios activos, ha comprado Instagram por 1000 millones de dólares y Whatsapp por 22.000 millones. Apple vende en un año 78,4 millones terminales, por 70,8 millones de la surcoreana Samsung y 56 de la firma china

¹¹ Friedman, T. *Gracias por llegar tarde: Cómo la tecnología, la globalización y el cambio climático van a transformar el mundo los próximos años*, Deusto, 2018, p. 53.

¹² Recuperado en <https://www.technologyreview.es/s/5655/tu-genoma-secuenciado-y-en-una-app-personalizada-para-tu-adn-por-999-dolares>

Huawei. Con ellos el crecimiento de datos personales que necesitamos para transformarnos de seres analógicos a seres digitales se ha multiplicado exponencialmente. Si antaño solo nuestro médico de cabecera conocía nuestros datos clínicos hoy lo conocen hospitales, laboratorios de análisis y Google si hemos recibido la analítica en una cuenta de Gmail (el servicio de correo superó los mil millones de usuarios activos al mes el año 2015) o Apple si tenemos una cuenta de *Icloud*. Pero volvamos a 2007.

Ese mismo año viajé a una conferencia internacional de inteligencia de datos en New York y leí una viñeta cómica: “*Google is your competitor*”. Los servicios de inteligencia y los detectives teníamos a un competidor mucho mayor que nosotros: Google. Yo creí que era simplemente un chiste, una forma de decirnos que la gente ya no contrataría a detectives porque podían encontrar ellos solos las respuestas. Me equivoqué. Para mí el buscador era, y es, una herramienta para localizar información. Pero tras su apariencia alegre, la adaptación diaria de sus logotipos y la gratuidad de su sistema se esconde, en un nuevo trampantojo, una realidad: cada vez que hacemos una búsqueda, cada vez que nos conectamos a un teléfono Android, cada vez que usamos Google Maps facilitamos los datos para que una empresa particular sepa nuestros movimientos, nuestras querencias y nuestras dudas. 2007 fue, en realidad, el año de la gran paradoja, del gran David Coperfield, el año en que cedimos nuestra privacidad a cambio de que un buscador nos facilitase el camino para adentrarnos en la nueva era, en Internet.

Me mantuve ajeno a la gran paradoja hasta 2015. Entonces cayó en mis manos un ensayo publicado en *London Review of Books* titulado ‘*The Robots are coming*’¹³. No sé si lo leí una o

¹³ Lancaster, J, *The robots are coming*, London Review of Books, Vol. 37, nº 5, March 2015.

varias veces, pero de lo que estoy seguro es de que entendí que el futuro me había arrollado. En España estábamos saliendo de la crisis económica y los problemas no nos dejaban ver más allá del horizonte analógico de nuestra cuenta bancaria. Entonces recordé la viñeta de Google y empecé a bucear sobre cómo el acceso y el análisis de datos había empezado a convergir en una muy cercana nueva revolución industrial. A golpe de clic conseguí libros, artículos y datos suficientes para empezar a pensar en una transformación de mi propio negocio. Pronto volví a pensar en Google y en cómo parecía el Galileo de nuestra era. Sabe de todo y de todos.

Yo, que me dedico a eso tan extraño de '*descubrir lo secreto y probarlo*', sé que las personas tenemos una faceta pública, una privada y otra secreta. Si Google es mi competencia, ¿qué faceta conoce la máquina de todos nosotros? Aparentemente, si es de acceso público sólo debería conocer datos de carácter público. Los detectives, qué no decir de las agencias de inteligencia, profundizan en dichos datos llegando a conocer algo así como la "*deep information*", esto es, la faceta privada, la información más profunda. ¿Qué ocurre entonces con los secretos? ¿Quién los conoce? Se lo diré. Hoy mi competencia es cada uno de nuestros smartphones y las grandes corporaciones tecnológicas. Aquel primer Iphone escondía, bajo su sencillez, un ordenador que, hoy tras el paso de los años y su evolución, conoce nuestras tres facetas, la pública, la privada y la secreta y quien pueda acceder a él sabrá nuestros anhelos más recónditos. Y, por eso, debemos convertirlo en una verdadera caja fuerte que únicamente facilite los datos a quienes nosotros debemos nuestro consentimiento. Un sistema, que como se verá, no ceda los datos, sino que los mantenga en un solo dispositivo y que, mediante, sistemas de consentimiento permita su acceso temporal. El ejemplo es sencillo: ya no realizaremos la declaración de la renta. Nuestros ingresos y gastos se almacenarán en nuestro

teléfono y no en el banco. Nosotros seremos los que permitamos al banco o a Hacienda que accedan al sistema, tomen los datos que requieran y autoricemos y, posteriormente, realicen la declaración dejando nuestros datos en nuestra caja fuerte, nuestro teléfono. Si no es así, en pocos años serán muchos los operadores los que conocerán nuestra personalidad digital y nosotros seremos esclavos de la tecnología.

Es la verdad. El siglo XXI es la era de la transformación digital y el de las respuestas sencillas a problemas complejos. Es la era en que las clases medias que conquistaron el mundo durante la Ilustración perderán su hegemonía. Sin fronteras, con dinero moviéndose en código binario, con la muerte prematura de la democracia liberal y la aparición de populismos y nacionalismos las empresas tecnológicas parece que podrán conquistar el mundo. El miedo ha aparecido en la sociedad y las dudas han absorbido nuestro pensamiento liberal. ¿Conseguirán los robots acabar con la clase media? ¿La Inteligencia Artificial acabará con la humanidad? ¿Los Estados nos convertirán en esclavos digitales sin privacidad? ¿Continúa vigente el pacto social con el que nos sociabilizamos desde la Ilustración?

Para Rousseau¹⁴ ese hombre primitivo del que he hablado al principio, diferente del socializado, vivía solo, ocioso y siempre rodeado de peligros, aunque sin violencia. Meramente dormía, jugada o cazaba. Éramos hombres libres hasta que entramos en sociedad. Nació el contrato social, el origen de la sociedad civil que surgió de la usurpación de las tierras. Nació la propiedad y con ella la contienda por acumulación de propiedades. Esta desigualdad, según Rousseau, trajo consigo al hombre socializado diferente del hombre natural. Cedimos parte de nuestra libertad, parte de nuestra intimidad a cambio de seguridad,

¹⁴ Rousseau, JJ. *El contrato social*. Taurus. 2012.

algo que fue palmario durante un Estado de Alarma y el cumplimiento, más o menos estricto, con el que sobrellevamos el confinamiento domiciliario.

Por eso ahora que hemos vuelto al primitivismo necesitamos retomar los estudios sobre la socialización. Debemos ponderar si vale la pena ceder alguna de nuestras libertades a cambio de seguridad en nuestra vida digital. Mi maestro, el profesor Morales Prats, señala que no podemos olvidar una ecuación básica de nuestra sociedad: sin orden no hay paz, sin paz no hay seguridad, sin seguridad no hay libertad y sin libertad no hay derecho al libre desarrollo de la personalidad. ¿Necesitamos cambiar el contrato social y permitir una cesión de nuestros derechos civiles a cambio de la seguridad sanitaria de nuestras vidas?

El poder de las corporaciones

La historia de la recolección de datos es la historia del nacimiento de Google. Larry Page y Serguéi Brin lanzaron su buscador en 1998. A finales ese año llevaban indexado dos millones y medio de webs. Anunciaron que iban a “organizar la información del mundo y hacerla universalmente accesible y útil”. Su código deontológico: “*Don't do Evil*” («no hagas el mal»). Su método: ofrecer servicios gratis a cambio de datos que son utilizados para mejorar el servicio. Sabiendo quién es el usuario podemos ofrecerle mejores resultados, es su lema. Y, naturalmente, mejor publicidad¹⁵.

Algunos hablan de una historia oculta, de un lado oscuro. “La estrategia de la objetividad —que Google actúa poniendo el acento en la investigación, en la excelencia académica, en la superioridad tecnológica, en el cuidado estudio de las interfa-

¹⁵ Marta Peirano, op. cit, p. 102.

ces— es un velo que oculta la inquietante perspectiva de un único punto de acceso a los datos producidos por los ingenios usuarios”¹⁶. Franklin Foer¹⁷ analiza las peculiaridades de cada gigante tecnológico (Google, Amazon o Facebook) en su libro “Un mundo sin ideas”. Nos previene de su capacidad para manipular la visión del mundo y condicionar la democracia. Nos explica cómo los algoritmos erosionan el libre albedrío y la creatividad. La riqueza de la información genera pobreza de atención.

El “efecto CNN” se ha descrito como la necesidad de información en tiempo real. Empezó con los bombardeos de Iraq, se aceleró con las Torres Gemenal y culmina por la necesidad acuciante de estar informado al minuto sin esperar a leer el periódico con el café de la mañana. Necesitamos el chute de información para paliar el miedo a lo que viene. La gente roba mascarillas en hospitales para ganar dinero con el coronavirus sin pensar que los pacientes oncológicos las necesitan de verdad. Y no lo hacen quinquis sino médicos o enfermeros. Estamos en una sociedad donde el miedo nos convierte en narcisistas patológicos. Y la información lo palia. También la indignación.

Indignados somos más fáciles. Parece una nueva paradoja, pero es cierta. Creemos que existe un derecho al insulto que nunca ha existido en la libertad de expresión. El odio, el miedo desaparece con el grito y el insulto. Las redes (Twitter) lo saben y lo fomentan. La indignación es la heroína de las redes sociales. “Genera más dopamina que ninguna otra cosa porque nos convence de que somos buenas personas y, encima, de que tenemos razón. Pensamos que tenemos pensamientos éticos cuando en realidad nos invade un sentimiento moral (...). Es un senti-

¹⁶ Ippolita. *El lado oscuro de Google*, Virus Editorial, 2010, p.104

¹⁷ Foer, F., *Un mundo sin ideas*, Paidós, 2017.

miento que nos define como personas buenas y que demanda justicia, venganza y mucha atención. Queremos compartir la llama con todas las personas del mundo para que sus sentimientos validen los nuestros con comentarios, likes y retuits. Que para el algoritmo de YouTube es simplemente generar *engagement*, su objetivo principal¹⁸. Nir Eyal¹⁹ defiende a las redes sociales y las compara con las novelas de antaño, “un entretenimiento de masas” al que se critica simplemente por el hecho de “ser nuevo”. Es posible que tenga razón. Nadie critica a una novela por ser “adictiva” en cambio se escriben libros contra los “videojuegos adictivos” como “empantallados”²⁰. Y el problema es precisamente eso: que las aplicaciones se crean bajo los mismos fundamentos que las tragaperras. Engancharnos. Nos dan droga a cambio de nuestros datos.

Ha llegado el momento de desarrollar “redes autónomas y descentralizadas para contraponer el deseo de «explorar» y «recorrer» las redes a la necesidad de «acceder» a los datos, para centrar la atención en el camino en lugar de en el resultado”²¹. Los gigantes tecnológicos dominan el mercado y, según Joseph Stiglitz, han conseguido aprovecharse de las “debilidades del individuo”²². Señala el nobel que, si una empresa conoce, por ejemplo, una personalidad adictiva podría bombardearnos con publicidad sobre máquinas recreativas o de viajes a Las Vegas. Su visión algo distópica no se confunde al señalar que si hay “grandes cantidades de datos en manos pocas empresas” eso sí tiene consecuencias para el mercado, la privacidad y la seguridad. Y también ocurre con algunas naciones.

¹⁸ Marta Peirano. El enemigo conoce el sistema, op. cit., p. 48.

¹⁹ Eyal, N., *Hooked: How to Build Habit-Forming Products*, Penguin, 2014.

²⁰ Moll, S y Faro, A, *Empantallados: como convivir con hijos digitales*, Larousse, 2017.

²¹ Ippolita. El lado oscuro de Google, op. cit.

²² Stiglitz, *Capitalismo progresista. La respuesta a la era del malestar*, op. cit. 130.

La magia china

En diciembre de 2019 China sucumbía al coronavirus que asoló el Planeta y se presentaba al mundo con un trampantojo de medidas tecnológicas contra la enfermedad que ocultaba la verdadera fórmula contra la pandemia: robots desinfectantes, cascos inteligentes, drones, cámaras térmicas y máquinas automatizadas que repartían comida eran una especie de estereograma, una ilusión óptima que ocultaba la verdadera solución: el control social mediante inteligencia artificial y “big data”.

Mientras con una mano nos enseñaban sus máquinas del futuro, con la otra creaban dos aplicaciones sencillas para frenar el contagio. Un semáforo digital en forma de aplicación para el teléfono celular dividió a la ciudadanía en rojo, para quien había estado en contacto con zonas afectadas; amarillo, para los que habían residido en zona de peligro; y verde, para quienes podían moverse con libertad. Una segunda aplicación permitió el monitoreo de los datos digitales de sus ciudadanos para determinar con quién se habían cruzado o mantenido relación. Finalmente, la policía y la propia ciudadanía mediante comités vecinales - que suenan a la Cuba castrista- controlaron a sus propios conciudadanos con tomas constantes de la temperatura corporal. Gran Hermano frenó la epidemia y sus ciudadanos parecen agradecidos. Pero el control social no es una vacuna ni un antídoto contra la covid-19. Es, simplemente, un medio para evitar la propagación al inicio de la infección que pretenden imponer a través de un pasaporte vital, una especie de carné por puntos ciudadano donde todos nacemos con las mismas libertades que vamos perdiendo a medida que nuestros vicios privados afectan a nuestra vida de bebés puros con el que a partir de ahora pretenden convivir. Estamos cada vez más cerca de la distopía del Gran Hermano orwelliano.

Tim Cook, CEO de Apple, siempre en guerra contra Facebook, manifestó en la Universidad de Stanford que “si aceptamos como normal e inevitable que todo en nuestras vidas puede ser agregado, vendido o incluso filtrado por una brecha de seguridad, entonces perdemos mucho más que datos. Perdemos la libertad de ser humanos”²³. Para Cook la privacidad es uno de los asuntos más importantes del siglo XXI sin darse cuenta de que paradójicamente en el mundo digital aceptamos la cesión de libertades que cercenamos en el mundo analógico, pero es en este segundo espacio donde la exposición al virus es real. Así, durante el coronavirus estuvimos encerrados analógicamente y libres digitalmente creyendo que en el ágora de los datos podíamos pasear más seguros que en las calles lastradas por el virus. Sin embargo, no nos damos cuenta de que al navegar por internet cedemos parte de nuestra privacidad a cambio de pequeñas píldoras de información gratuita. Google conocía antes que los gobiernos si estábamos infectados. En el mundo terrenal preferimos enfermar a estar controlados, a pesar de que, en Estados Unidos, frente a los riesgos terroristas se crearon leyes como la Patriot Act, que ocultan la misma cesación de libertades a gran escala que rige en China. Es la paradoja de la privacidad que deberá resolverse en un futuro contrato social.

Nos hemos dissociado en dos personalidades, la digital y la analógica. A partir de ahora el derecho deberá protegernos corporal y digitalmente y en ambos mundos la privacidad tendrá un significado tan dispar como las medidas que deberemos tomar para poder seguir siendo libres. En pocos años los Estados de Europa deberán determinar si durante los futuros estados de alarma, que seguramente llegarán, deberemos ceder parte de nuestros derechos a cambio de confinar a la pandemia y no de confinarlos en nuestras casas. Es el momento de estudiar si el

²³ Recuperado en Apple CEO Tim Cook Stanford commencement speech (cnbc.com)

control social analógico mediante herramientas digitales será (o no) necesario al inicio de la propagación de un nuevo virus y no cuando la enfermedad asole nuestros países. Con todas esas preguntas y reflexiones inicié este estudio cuyas conclusiones son halagüeñas sin conseguimos domeñar a las grandes corporaciones tecnológicas. Les doy una pista: la clave está en los datos de carácter personal y la solución el contrato social. Bienvenidos al futuro.



❖ CAPÍTULO 2. HACIA LA SOCIEDAD HIPERINDIVIDUALISTA

Ontológicamente, el hombre necesita relacionarse, comunicarse y vivir en sociedad. La mera convivencia produce una evolución en la lengua, en el trato y en la protección social. Sin embargo, como les he dicho, la comunicación digital, la vida a través de una pantalla, nos ha convertido en seres individualistas. La sociedad actual ha cambiado. Buscamos sentirnos diferentes y especiales, no ya a través de la propiedad sino de la imagen. Hemos entrado en un proceso de individualización. Para la psicología se trata de un proceso donde el hombre desplaza sus afectos y relaciones de la familia al grupo. Para la sociología es una nueva forma de relación en la que el mundo se centra en uno mismo. El derecho debe, por tanto, centrar su intervención en la protección del individuo.

Parece que el hombre actual es similar al primitivo en su propia soledad e individualización. Cabe preguntarse, entonces, si hoy en día es necesario el “contrato social” que en origen el hombre no necesitó en su soledad de pastor. En su primera formulación, aquellos hombres primitivos y pobres vendieron su libertad a cambio de seguridad y se convirtieron en esclavos feudales. Para solventarlo Rousseau formuló un segundo contrato social que organizaba al conjunto sin renunciar a la libertad. Se trataba de “encontrar una forma de asociación que defienda y proteja con la fuerza común, la persona y los bienes de cada asociado y por lo cual cada uno, uniéndose a todos los demás, no obedezca más que así mismo y permanezca, por tanto, tan libre como antes”²⁴, señaló el filósofo. Bajo esas premisas hoy

²⁴ Rousseau, JJ. *El Contrato Social*, op. cit., p.27

podemos afirmar que los hombres convivimos bajo la tutela de los derechos y las obligaciones, renunciando a parte de nuestra libertad propia del individuo. Esos derechos son las cláusulas del contrato social y, a su vez, sus límites para preservar la convivencia que marcamos con el pacto civil. Algo que Internet puso patas arriba, a pesar de que lo advirtió Benjamin Franklin: “aquellos que sacrifican la libertad por seguridad no merecen tener ninguna de las dos”²⁵.

El Presidente de los Estados Unidos, Barack Obama, en su toma de posesión rechazó como falsa, que tengamos que elegir entre la seguridad y los ideales. “Nuestros padres Fundadores, enfrentados a peligros que apenas podemos imaginar, elaboraron una carta que garantizase el imperio de la ley y los derechos humanos”²⁶, dijo en aquel discurso que ha pasado a los manuales de ciencia política. Es cierto, la revolución tecnológica de Internet supuso una nueva conquista del Oeste americano. Una nueva usurpación de tierras, un nuevo brote de violencia por la propiedad, una nueva acumulación de riqueza. Internet, sin embargo, no tuvo más remedio que adaptarse al medio del contrato preexistente. ¿Por qué ahora deberíamos abogar por un nuevo contrato social? Estamos a las puertas de una 5ª revolución tecnológica: la transformación digital. Algunos señalan que si se estudia en profundidad a las sociedades más digitalizadas nos asomaremos a una suerte de nuevas dictaduras que provocan la cesión de los derechos individuales en aras a la conectividad social. ¿Tenemos entonces a hombres encerrados en su individualidad cediendo sus derechos? ¿Estamos ante un nuevo primer contrato social donde el hombre pastor aceptó su esclavitud ante el poder del terrateniente?

²⁵ Citado en Ayllon Santiago, H y Fernández González, CM, *Tratamiento de datos de carácter personal en el ámbito policial*, Reus Editorial, 2021.

²⁶ Obama, B., recuperado en El arduo dilema ideales-seguridad | Opinión | EL PAÍS (elpais.com).

Hacia la nueva esclavitud y la transformación social

Existen en la actualidad multitud de grupos en defensa de los derechos civiles que claman por una hiperprotección del derecho a la privacidad sin entender que no estamos ante un nuevo contrato social como tal, sino ante una evolución del preestablecido por Rousseau en el ámbito analógico y uno totalmente nuevo en el ámbito digital. En aquel, los individuos cedíamos parte de nuestra libertad a cambio de seguridad (policía) y, en la actualidad, debemos ceder parte de nuestra privacidad a cambio de una tecnología segura. El ejemplo es sencillo y lo encontramos en las tarjetas de crédito. Su origen se remonta a 1914 cuando la empresa Western Union crea una tarjeta para sus clientes preferenciales, facilitándoles una línea de crédito sin cargo. Con posterioridad, catorce restaurantes neoyorquinos unieron fuerza y crearon el Diners' Club. Su modelo de negocio se basaba en hacer de intermediario entre el establecimiento y el comprador, cobrando una comisión por transacción al primero y una comisión de mantenimiento (3 dólares anuales en 1951) al segundo, a cambio de un pago aplazado a final de mes sin intereses. Con el éxito llegaron otras tarjetas y los fraudes. Llegó la digitalización y las interminables horas para que el sistema aceptase nuestra tarjeta. La sociedad demandó seguridad y rapidez. El único sistema fue la unificación de datos crediticios que, consultados por el sistema, autorizaban el pago. Cedimos privacidad a cambio de seguridad y rapidez. La misma intimidad que hoy reclamamos y que nuestros antepasados han reclamado en cada transformación social.

La máquina de vapor, la electricidad, la producción industrial y la tecnología digital han sido los hitos que han encendido cuatro revoluciones industriales. Y estábamos intentando entender la cuarta cuando ha llegado la quinta: la digitalización y la inteligencia artificial. “Estamos al borde de una revolución tecno-

lógica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes”, vaticina Klaus Schwab, economista alemán y fundador del Foro Económico Mundial autor del libro “La cuarta revolución industrial”, publicado en 2016²⁷.

Los datos y el *big data* serán el centro del cambio que modificará el mundo tal y como lo conocemos. Los avances en los campos de la robótica, de la inteligencia artificial, de la nanotecnología, de la biotecnología, de la computación cuántica, del Big Data, de la impresión 3D y de los vehículos autónomos, según Schwab, serán el pivote sobre los que se erigirá el cambio más importante que ha sufrido la humanidad. Esta revolución determinará “el mercado del empleo, el futuro del trabajo, la desigualdad en el ingreso”²⁸ y la ética del individuo estará en el eje de los límites del derecho. El darwinismo tecnológico afectará sobremanera a la empresa 4.0 y provocará desigualdades hasta ahora nunca vistas. Pero no es nada diferente a lo que ocurrió a finales del siglo XVII en Francia y que culminó con la Revolución Francesa. Acababa la prosperidad de Luís XIV y empezaron a relajarse las costumbres aumentando la corrupción y decayendo la autoridad del Gobierno. Entonces surgió la Ilustración y el cambio más importante que ha sufrido la humanidad hasta que la 5ª revolución industrial nos devore.

¿Qué es la Ilustración? Immanuel Kant responde en el artículo «Respuesta a la pregunta ¿Que es la Ilustración?» que consiste en “la salida de la humanidad” de su “minoría de edad” y de su

²⁷ Schwab, K, *La cuarta revolución industrial*, Debate, 2016, p. 175.

²⁸ Schwab, K, *La cuarta revolución industrial*, op. cit. 201.

“sumisión a los dogmas” de las autoridades religiosas y políticas²⁹. El Gobierno dejó su manto de divinidad y pasó a ser una mera convención humana. Dejamos el absolutismo en favor de la democracia y las leyes lejos de ser una imposición divina devinieron en una suerte de justicia de los hombres abandonando los pecados a la confesión eclesiástica³⁰. Sea como fuere, señala la doctrina³¹, “no cabe duda de que el siglo ilustrado es el siglo del triunfo del hombre y sobre todo de su razón autónoma como instrumento para llegar al conocimiento de todas las cosas. Es la centuria de los grandes descubrimientos, de los grandes avances tecnológicos y, sobre todo, de la revolución en el conocimiento de la naturaleza, concepto éste presente a lo largo de toda la filosofía ilustrada”. El hombre pasa de la oscuridad a la luz, la luz de la razón. En palabras de Weiland³², “la luz del espíritu, de la que aquí se habla, es el conocimiento de lo verdadero y de lo falso, de lo bueno y de lo malo”. La luz es la razón frente a la superstición. Es la época del progreso y de la evolución. Diderot escribe a Voltaire “los otros historiadores nos narran hechos para darnos a conocer hechos. Usted, para suscitar en el fondo de nuestras almas una indignación profunda contra la mentira, la ignorancia, la hipocresía, la superstición, el fanatismo, la tiranía, y esta indignación permanece cuando ha pasado la memoria de los hechos”³³. Allí empieza la evolución y ahora no la pudimos parar. Como tampoco podemos impedir que llegue la nueva revolución: la de la persona digital y su personalidad jurídica.

²⁹ Kant, I, *¿Qué es la Ilustración?*, Alianza Editorial, edición de 2013.

³⁰ Pinker, S, *En defensa de la Ilustración: Por la razón, la ciencia, el humanismo y el progreso*, Paidós, 2018.

³¹ Cristóbal de Gregorio, J., Los ilustrados y la Ilustración, en BFD: Boletín de la Facultad de Derecho de la UNED, N° 8-9, 1995, págs. 125-146

³² WIELAND, «Seis preguntas sobre la Ilustración», en A.A.V.V, *¿Qué es Ilustración?*, Tecnos, Madrid, 1988

³³ Diderot citado por Cristóbal de Gregorio, J., Los ilustrados y la Ilustración, op. cit.

La doble personalidad jurídica: identidad 2.0

Hoy en día, nada más nacer, tenemos personalidad jurídica. Este hecho, aunque pueda parecer un asunto menor, no lo es, ya que nada más nacer tenemos derechos y obligaciones, algo fundamental, por ejemplo, en materia hereditaria. Pues bien, permítanme que adelante una parte de las conclusiones de este estudio. En la revolución industrial que viene, en la transformación digital del mundo, cuando nazcamos lo haremos con dos personalidades: una la analógica, la de siempre, la que ya conocemos y el Código Civil reconoce en su artículo 30: “La personalidad se adquiere desde el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno”. Otra, la digital, que nacerá en el mismo momento que el médico corte el cordón umbilical, la matrona haga las comprobaciones fisiológicas o tome las huellas dactilares y las transmita digitalmente. A partir de esos momentos los datos del bebé pasarán a un sistema informático con valor económico sino lo estaban antes de nacer al estar en la base de datos de la ecografía 3D. Y ese será su primer sueldo, porque todos nacemos con un pan bajo el brazo. Esos datos acabarán en una especie de urna digital que a modo de cartilla bancaria generará ingresos y gastos. Todo ello formará parte de una nueva identidad digital que debe regularse.

En Internet la identidad no es la misma que en el mundo analógico, eso parece claro a ojo de un ciudadano medio. Nuestra personalidad real difiere de la identidad digital, porque son diferentes. Un documento de trabajo de BBVA Research define la identidad digital como “el conjunto de atributos que vinculan una entidad personal con sus interacciones online”. Y destaca: “lo que es realmente importante es la validación que otros hacen de los atributos que compartimos para demostrar nuestra

identidad en la red”³⁴. Es decir, la capacidad de probar que somos analógicamente quienes decimos ser digitalmente.

La identidad digital es la versión de los datos recopilados en Internet de una identidad física. Considero que, sin embargo, cuando usamos una mera identidad digital para identificarnos con la Administración (o una entidad bancaria) es la mera traslación de nuestra personalidad analógica. Lo verdaderamente importante, a los efectos de este trabajo, es comprobar que nuestra identidad digital es diferente de nuestra identidad analógica cuando no necesitamos identificarnos y, simplemente, navegamos por Internet. Estamos frente a un escaparate digital donde nos presentamos como queremos. La Identidad Digital es, por tanto, el conglomerado de informaciones que hay en Internet y que componen la imagen que los demás tienen sobre nosotros. Hablamos, por tanto, de una “identidad expandida” a través de los “datos derivados” que recopilan terceros. Somos lo que decimos que somos y otros ven de nosotros.

Ahí radica el problema fundamental: hemos dejado de ser nosotros mismos para depender de lo que los demás creen que somos. Ya no somos lo que somos sino lo que los demás perciben de nosotros. Según Aparici y Osuna³⁵, ‘Identidad 2.0’ o ‘identidad digital’ es todo lo que manifestamos de nosotros mismos en el ciberespacio e incluye tanto nuestras actuaciones como la forma en la que nos perciben los demás en la red. Nuestro correo electrónico, nuestra página de LinkedIn, las noticias publicadas sobre nosotros o nuestra página de Instagram configuran un todo que determina nuestra identidad digital y que, en muchos casos, difiere de la realidad.

³⁴ Segovia A y Martín A, Digital identity: the current state of affairs recuperado en Digital Identity: the current state of affairs (bbvaresearch.com)

³⁵ Aparici, R. y Osuna Acedo, S. (2013). La Cultura de la Participación. Revista Mediterránea de Comunicación, vol. 4, nº 2, 137-148

En este sentido, hace poco un personaje público, cansado del acoso al que le sometían subiendo a las redes fotografías de su vida analógica, nos solicitó a un grupo de expertos jurídicos que ideásemos una acción que le permitiese abortar esos ataques. Llegamos a la conclusión de que lo único que funcionaría es lo que se conoce como acción de jactancia (“La acción de jactancia tiene lugar cuando hay una ostentación pública, por parte del jactancioso, contra un tercero, de una pretensión jurídica, ocasionándole al tercero un perjuicio jurídico, económico o moral. La acción de jactancia sería el recurso que el derecho ofrece al perjudicado frente a tal daño; concretamente la acción judicial para obligar al jactancioso a ejercer la pretensión jurídica ostentada o, en caso contrario, imponiéndole el silencio perpetuo”)³⁶ o una querrela por stalking o acoso³⁷ contra la identidad digital acosadora. Pero nada funcionó porque intentábamos luchar en el mundo digital con herramientas del mundo analógico. El acosador podría cambiar de identidad digital al momento y continuar con su actividad sin problema.

La identidad digital es, por tanto, la traslación de la identidad física al mundo online que integra lo que decimos que somos y lo que los algoritmos perciben de nosotros. Podemos crear tantas versiones digitales como queramos de nuestra identidad real. En Internet puedo ser Francisca sin problemas, pero los algoritmos detectarán que, en realidad, soy Francisco Marco analógico. Es más, por mi trabajo, tengo diversas identidades digitales que utilizo para obtener información, pero sólo una identidad real (la personalidad digital) cuando me identifico frente a la Administración Pública o mi entidad bancaria. Mi

³⁶ Muñoz Perea, D. La acción de jactancia en el derecho civil actual. Recuperado en La acción de jactancia en el derecho civil actual · Noticias Jurídicas (juridicas.com)

³⁷ El stalking o acecho, Consiste en acosar a una persona de forma insistente y reiterada, de manera que le produzca una alteración grave en el desarrollo de su vida cotidiana, es decir, debe tratarse de algo más que meras molestias, obligando a la víctima a variar sus hábitos cotidianos como única vía escapatoria.

identidad digital ya no se fundamenta en rasgos físicos o documentales sino en mi forma de relacionarme en el mundo digital. Formo parte de una sociedad analógica y todas mis identidades forman parte de la Sociedad Digital. Y en esta nueva Sociedad mi identifico con los datos que he ido diseminando en el mundo digital que son de fácil acceso por lo que parece claro que la gestión que se haga de dichos datos (gestión de la privacidad) será fundamental.

El derecho de los datos

Como se verá a lo largo de este trabajo debemos desterrar (en el mundo digital) el concepto de “propiedad sobre los datos” para transformarlo en el “derecho sobre los datos”. Estamos en una era donde “nuestro yo digital está siendo perfilado, agregado y reducido a código para que las organizaciones se dirijan a nosotros como sujetos de consumo (Pridmore & Lyon)” y debemos ser nosotros mismos quienes determinemos quién tiene derecho sobre nuestros propios datos. Lo sé, es difícil adelantarse al tiempo o ser Nostradamus, pero el derecho es así y debe preparar propuestas de *lege ferenda* que permitan a la humanidad adaptarse a los nuevos tiempos, más en el juego del desarrollo, donde siempre hay perdedores. Elizabeth Garbee, investigadora de la Escuela para el Futuro de la Innovación en la Sociedad de la Universidad Estatal de Arizona, señala que “hay un real riesgo de que la élite tecnocrática vea todos los cambios que vienen como una justificación de sus valores. Ese tipo de ideología limita gravemente las perspectivas que se traen a la mesa a la hora de tomar decisiones (políticas), lo que a su vez exacerba la inequidad que ya vemos en el mundo hoy”³⁸.

³⁸ Citado en Perasso, G. (2016N). ¿Qué es la cuarta revolución industrial? BBC Mundo 12/10/2016. Recuperado de <http://www.bbc.com/mundo/noticias-37631834>

No permitamos que eso ocurra y que algunos ganen con lo que nosotros regalamos. Por eso, el modelo de contrato social que se elija es tan importante.



❖ CAPÍTULO 3. HACIA UN NUEVO CONTROL SOCIAL EN LA ERA DIGITAL

La necesidad de controlar Internet es tan acuciante que ha provocado una guerra comercial entre China y Estados Unidos. La OTAN, la Unión Europea y Estados Unidos han acusado sistemáticamente a China de provocar ataques informáticos globales para controlar la red. Según informes del FBI³⁹, China ha creado un ejército de 180.000 ciberespías para controlar al resto de países. Y todo ello tiene mucho que ver con el modelo de contrato social que rige territorialmente aquel país, tal y como comprobaremos.

Sin embargo, de forma previa a dicho estudio, se debe indicar que sea como fuere el contrato social, sea como fuere la relación entre el Estado y el ciudadano lo único seguro es que frente a la transformación digital y la disociación de nuestra personalidad jurídica debemos adentrarnos en un contrato social homogéneo digitalmente, es decir, un contrato social válido para cualquier sociedad, sustentado en la seguridad y la confianza, porque en Internet únicamente existe un sistema de vida. Debemos observar el presente con el conocimiento de los errores del pasado y la previsión de lo que ocurrirá en el futuro. El progreso de la humanidad, como he dicho, comenzó con la Ilustración y el posicionamiento de la razón como instrumento esencial para alcanzar la verdad dejando atrás las tradiciones y las supersticiones. El liberalismo y la revolución industrial ayudaron a extender desde las élites al pueblo el conocimiento y la igualdad. El contrato social fue el sustrato sobre el que se sustentaron aquellos avances que generaron igualdad, riqueza y conocimiento.

³⁹ Recuperado en [Cyberwar Rhetoric Is Scarier Than Threat of Foreign Attack](#) | Op-Ed | US News

El Estado pasó a ser el garante de los derechos y libertades del hombre. La humanización de las penas centró el discurso del derecho penal en cuanto el hombre se posicionó frente al absolutismo y la nobleza. Los derechos sociales que aquella Europa creó siguen siendo, en buena parte, el fundamento de nuestra sociedad que, entonces, avanzó con la burguesía y que hoy parece un museo reacio a la evolución.

Las conquistas sociales nos convierten en esclavos de los requerimientos que se exigen. Pretender demandar seguridad policial sin dotar a las Fuerzas y Cuerpos de Seguridad del Estado de capacidad de investigación es *strictu sensu* un imposible. Solicitar velocidad en las comunicaciones digitales sin que la red nos identifique y, por tanto, nos individualice y nos rastree es una utopía imposible de acometer. Otra cosa es establecer los límites de la conquista, algo que se le debe exigir a la colectividad representada por el Estado Social. Los individuos no podemos demandar intimidad y seguridad sin cesiones. Eso sería tanto como pedir derechos sin tener obligaciones, algo que está en la pura esencia del contrato social. Por eso, la lógica nos pide que analicemos las demandas sociales de aquellos que exigen un nuevo contrato social en la era digital válido en todo el planeta (en internet) y por tanto muy difícil por cuanto los contratos sociales son diferentes según los territorios.

Hacia un contrato social digital

Según la Declaración Deusto Derechos Humanos en Entornos Digitales de 26 de noviembre de 2018 la transformación digital es irremediable. Oponernos a la tecnología es un debate irrelevante y debemos centrarnos en un único objetivo: la evolución social y la vuelta a las doctrinas antropocéntricas del humanismo. Ya en el siglo XVIII, David Hume examina las tesis del pacto social en que se basa el contractualismo: “Los hombres

cambian su libertad natural por las leyes para obtener paz y orden; es decir, por seguridad”⁴⁰. La prioridad debe ser el ser humano. Para mantener el contrato social, debemos regular con un doble objetivo: impedir que exista un monopolio de datos y se garantice la seguridad de estos. Las medidas de seguridad (confianza) serán el motor del contrato social junto al consentimiento informado.

El ya fallecido filósofo israelí David Hartman, según narra Thomas Friedman⁴¹, explicaba que el ciberespacio se parece al mundo del que hablaban los profetas “un lugar donde toda la humanidad puede estar unida y ser totalmente libre”. Sin embargo, añade: “el peligro es que estamos uniendo a toda la humanidad en el ciberespacio, pero sin Dios”. Es cierto, cada vez más nos acercamos a un mundo sin fronteras, valores y leyes que se parece al verdadero país único. Un mismo espacio donde nos reunimos 4.540 millones de personas⁴² de los 7700 millones de personas que las conformamos la población mundial según Naciones Unidas. La penetración de Internet pronto alcanzará cifras cercanas al 90% de forma global.

Estamos en una era donde las aceleraciones han provocado que pasemos de una monocultura a una policultura (Friedman) lo que supone disrupciones y miedos. Cambian las convenciones sociales, se hablan lenguas extranjeras, se adoptan religiones y vestimentas y su uso genera problemas sociales, políticos y legales. Todo está cambiando en el mundo analógico a medida que el mundo tecnológico invade nuestra vida. El concepto de familia ha cambiado, los roles de hombre y mujer se han traspasado y ha vuelto, de forma clara, la individualidad frente al co-

⁴⁰ Citado en Pacto social, Constitución y democracia, ¿game over? (infolibre.es)

⁴¹ Friedman, T., *Gracias por llegar tarde: Cómo la tecnología, la globalización y el cambio climático van a transformar el mundo los próximos años*, op. cit.

⁴² Digital 2020 Global Digital Overview (January 2020)

lectivismo. Nuestra forma de ver la vida ha pasado de la venta a la pantalla del smartphone. La lengua se estanca con las apócope y la escritura disfuncional de los mensajes. No hablamos y nuestra imagen se ha convertido en el centro del universo digital. Ello ha provocado que la clase media se sienta a la deriva. Trump, el Brexit, Vox y los nacionalismos ha surgido de esta deriva. Y a todo eso le debemos añadir el miedo al progreso, el miedo a la pérdida de trabajos por culpa de las máquinas y a la creciente certeza de que el Gran Hermano de Orwell está por llegar. Miedos que aparecen guiados por los medios de comunicación ávidos de titulares de “hombre muerde a perro”.

El año 2007 empezó todo, como he dicho al principio de este trabajo y la Ley de Moore no ha fallado (aproximadamente cada dos años se duplica el número de transistores en un microprocesador). Las tecnologías físicas han seguido creciendo sin parar, pero las tecnologías sociales no han crecido al mismo ritmo. En 2008 el mundo entró en recesión y por culpa de su descentralización cada comunidad luchó individualmente. “En consecuencia, hemos visto que muchas de nuestras tecnologías físicas superaban trabas, mientras que nuestras tecnologías sociales -educación, gobierno y regulación- se atascan”⁴³, lo que ha provocado que muchas sociedades se sientan a la deriva. España, como en la Ilustración, parece querer encabezar el vagón de segunda velocidad. China, sin contrato social, parece el ganador.

Y solo tenemos una solución: adaptarnos a toda velocidad. Es más, la descentralización está generando trabas. ¿Cómo? Con cada revolución industrial o giro económico “una nueva clase de activo se convierte en la base principal de crecimiento de la productividad, creación de riqueza y oportunidades”). En la economía agraria el activo era la tierra, en la industrial el capital

⁴³ Friedman, J., op. cit., p. 60

físico, en la de servicios los “activos intangibles” (métodos, diseños, software, etc) y en la nueva era será “el capital humano: talento, capacidades, empatía y creatividad”⁴⁴. Estamos por tanto ante la era del hombre. En el nuevo humanismo.

El nuevo humanismo

El movimiento humanista del siglo XIV sentó las bases del derecho y de las políticas de derechos humanos actuales. El pensamiento humanista, como doctrina antropocéntrica, considera que la organización de la sociedad debe buscar el bienestar del hombre en su conjunto. Hoy debemos retornar al humanismo.

La Declaración de Independencia del Ciberespacio presentado en Davos (Suiza) el 8 de febrero de 1996 por John Perry Barlow, fundador de la *Electronic Frontier Foundation* (EFF) se promovió como respuesta a la *Telecommunication Act* en los Estados Unidos afirma: “Estamos creando nuestro propio contrato social. Esta autoridad se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente. El ciberespacio está formado por transacciones, relaciones y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos. (...) Debemos declarar nuestros “yo” virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extendemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos. Crearemos una civilización de la mente en el ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes”⁴⁵.

⁴⁴ Citado en Friedman, op. cit., p.70.

⁴⁵ Recuperado en Microsoft Word - 5D7FD980.doc (uhu.es)

Más allá del “utopismo ácrata” de Barlow⁴⁶ y su oposición a cualquier regulación debemos centrarnos en su visión del nuevo yo virtual. Es el inicio de lo que vengo a defender: la creación de una nueva personalidad digital que debe ser regulada universalmente. Actualmente “se alzan diversas voces que hablan de la necesidad de construir un nuevo contrato social que establezca las pautas de comportamiento de la nueva civilización que estamos alumbrando a partir de la presente revolución digital”, señala Daniel Tornero⁴⁷. Pero ello es casi imposible si se pretende hacerlo territorialmente y materializar un único contrato social para la personalidad analógica y la digital ya que los diversos contratos sociales existentes son tan difíciles de aquilatar como la guerra comercial entre China y Estados Unidos.

El no contrato social en China

La economista y estudiosa de las finanzas globalizadas Loretta Napoleoni escribe en *Maonomics* que el modelo chino de contrato social se fundamenta en llegar a un acuerdo con los ciudadanos similar al siguiente: “muy bien, estamos aquí para gobernar con tu consenso y por tu interés, haciendo las cosas como tú quieres; no quieres democracia, quieres el bienestar económico y una buena vida, y nosotros nos ocupamos de todo”⁴⁸. El nuevo contrato social chino consiste en que el gobierno promete y garantiza a la población el crecimiento económico, que supone una mejora del bienestar social y la buena vida, y por lo que se refiere al ámbito político la población lo deja en manos del gobierno. Por otro lado, el ciudadano chino considera que el Estado está obligado a protegerle. Frédéric Bobin,

⁴⁶ La revolución digital requiere un nuevo contrato social (theconversation.com)

⁴⁷ Tornero, D. *Hacia un nuevo contrato sociodigital*, en *Hacia un nuevo contrato sociodigital* | Telos Fundación Telefónica (fundaciontelefonica.com)

⁴⁸ Napoleoni, L. *Maonomics: La amarga medicina china contra los escándalos de nuestra economía*, Paidós, 2011.

especialista en temas chinos de *Le Monde*, estudia cómo el Partido Comunista ha logrado mantener su legitimidad ante el pueblo chino, basada en dos elementos: la eficacia económica y el patriotismo.⁴⁹

En China fijaron su mirada en el comunismo de la ex Unión Soviética y asumieron que debían cambiar y abrir el sistema económico, pero mantuvieron el control político. Por eso en China no hay un derecho constitucional de protección de la *privacy* reconocido como tal, aunque en el capítulo segundo de su carta magna se mencione como un derecho fundamental de la ciudadanía. Ello es, principalmente, por dos motivos: el concepto de familia y el concepto de seguridad.

En nuestra cultura el castigo se basa en el concepto de culpa del cristianismo. Sin embargo, en la cultura china el castigo deriva de conceptos basados en las ideas confucianas de vergüenza y jerarquía. En China las acciones del individuo se reflejan en su apellido y posición en la comunidad. El concepto de vergüenza pública está por encima de cualquier expresión de culpa personal. La palabra tradicional china para "privacidad" es "yin-si". "Yin-si" está formado por dos palabras chinas, que son "yin" y "si". "Yin" significa "escondido". "Si" significa "privado" o "no quiero divulgar en público". "Yin-si" se ha definido como el secreto vergonzoso de un individuo y que el individuo no quiere que otros conozcan⁵⁰. La crítica de la comunidad está por encima de los deseos individuales. Por tanto, el bien colectivo está por encima del individual. Y no existe intimidad de grupo dado que el concepto requiere individualidad que el Estado rechaza.

⁴⁹ Bobin, F, *Le nouveau contrat social chinois*, recuperado en *Le nouveau contrat social chinois* (lemonde.fr)

⁵⁰ Tiffany Li, Zhou, Z, Bronfman, J, Saving Face: *Unfolding the Screen of Chinese Privacy Law*, *Journal of Law*, August, 2017.

Lo anterior permite que China sea la nación más vigilada con 200 millones de cámaras de videovigilancia (la siguiente es USA con 50 millones). Ocho de las diez ciudades más videovigiladas del mundo están en China⁵¹. Con 2.580.000 cámaras para controlar a 15.350.000 personas (una cámara por cada seis habitantes) Chongqing tiene más cámaras de vigilancia por habitante que ninguna otra ciudad del mundo, por encima incluso de Pekín, de Shanghai y de la ciudad tecnológica de Shenzhen, con capacidad de lectura las matrículas de los coches y la policía lleva unas gafas capaces de detectar biométricamente a los delincuentes. Los ciudadanos ceden su intimidad a cambio de seguridad⁵². Pero el Gobierno chino ha dado un paso más allá poniendo en marcha un sistema de rating ciudadano. Rongcheng fue la ciudad escogida para hacer una prueba piloto. Personas y empresas empiezan con mil puntos, que se traducen en un sistema de calificación de la 'A' a la 'D'. Los puntos se añaden por servicios a la comunidad, comportamientos excepcionales y premios recibidos. La resta puede producirse por no ceder el paso a los peatones hasta por retrasarse con el pago de las facturas o tener una multa de tráfico⁵³. Gracias al nuevo método puesto en marcha, el Estado recibe y gestiona grandes volúmenes de información obtenida en colaboración con bases de datos policiales e instrumentos de alta tecnología, como las gafas de reconocimiento facial. Un mes después de su puesta en marcha, ciento sesenta y nueve personas perdieron el derecho a viajar dentro y fuera del país por su baja puntuación⁵⁴. Otras consecuencias son la denegación de

⁵¹ Citado en Dos millones y medio de cámaras convierten la ciudad china de Chongqing en la más videovigilada del mundo (eldiario.es)

⁵² Con información de Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled | Cities | The Guardian

⁵³ Con información de Andrea Rodríguez en El sistema de crédito social chino - El Orden Mundial - EOM

⁵⁴ <https://www.scmp.com/news/china/policies-politics/article/2148980/china-names-169-people-banned-taking-flights-or-trains>

reservas en los mejores hoteles⁵⁵, pérdida de empleos e, incluso, de mascotas⁵⁶.

En Occidente damos por sentado que las tecnologías nos liberan y homogenizan y democratizan el poder. Sin embargo, en China, como en una novela distópica, se permite la censura y que el acceso a la información sea una utopía, algo que para algunos⁵⁷ supone una gran ventaja sobre los demás países. Es el contrato social del azúcar. Dopamina en forma de seguridad a cambio de la privacidad tanto analógica como digital. Nadie escapa al control chino ni analógico ni digital y sus ciudadanos, aparentemente, son felices y pueden gastar cientos de miles de euros en bolsos de marca en Occidente.

El contrato social individualista de los norteamericanos

En Estados Unidos la lejanía del individuo frente al Estado es consustancial a su formación como país. Ciudadanos de todos los lugares del mundo conquistaron la tierra, la usurparon y conformaron un nuevo país donde el individuo se situaba frente al Estado. La filósofa rusa afincada en Estados Unidos, Ayn Rand, define bien las diferencias culturales entre Europa y Estados Unidos en una de sus entrevistas: “La cultura europea adora al Estado porque está empapada de altruismo y autosacrificio y de la idea que el hombre debe existir por otros, y por lo tanto el mayor honor con que un europeo puede soñar es servir al Estado, o ser recompensado por el Estado. El Estado siempre es considerado como un ser casi sobrenatural, y el europeo es sólo un siervo. En América es exactamente lo contrario. La recompensa del esfuerzo individual y el liberalismo

⁵⁵ <https://www.bbc.com/news/world-asia-china-34592186>

⁵⁶ <http://uk.businessinsider.com/china-dog-owners-social-credit-score-2018-10?IR=T>

⁵⁷ Stiglitz, J. *Capitalismo progresista: La respuesta a la era del malestar*, Taurus, 2020.

frente al control estatal preside su forma de ver la vida y su contrato social”⁵⁸.

La conquista del Oeste es un hecho histórico fundamental en el nacimiento y desarrollo de los Estados Unidos que los historiadores consideran como el sustrato de su acusado individualismo. Pero no olvidemos que, finalmente, al sanguinario conquistador se le destierra en favor del granjero. La vieja ley de los conquistadores se sustituye por un Estado Moderno basado en el poder del consenso donde el individuo no está acogotado por el Estado. La constitución de los Estados Unidos es una parte bastante explícita del contrato social de este país. Dicta lo que el gobierno puede (o no) hacer. Las personas que eligen vivir en los EE. UU deben estar de acuerdo con lo que estipula la Constitución en cuanto a las obligaciones sociales y morales y ceñirse a la letra de su texto. Saben que el Estado no puede marcar el rumbo de sus ciudadanos, solo el esfuerzo es capaz de darles lo que el sueño americano ofrece. Por eso, en Estados Unidos no existe una legislación federal que proteja los datos de los usuarios y la privacidad equiparable a la normativa europea de protección de datos de carácter personal. Solo existen normativas sectoriales que regulan diferentes ámbitos⁵⁹.

Ese egoísmo cultural va más allá. Los ciudadanos nos damos la mano por influjo de los países sajones, era una forma de evitar el contacto físico. Alejamos a la persona de nuestro espacio personal y evitamos saludos más cercanos como los besos. Las normas no deben cercenar la capacidad del ciudadano para decidir que ceden de esos derechos que tienen en potencia somos nosotros, como en el “shake hands” quienes alejamos al otro o lo

⁵⁸ Recuperado en Objetivismo.org (webstarts.com)

⁵⁹ Como, por ejemplo, la Ley de Protección de la Privacidad de Menores de los Estados Unidos (CO-PPA), la Ley de Transferencia y Responsabilidad del Seguro Médico en EE. UU. (HIPAA) o la Ley de Cumplimiento Fiscal de Cuentas en el Extranjero (FATCA).

acercamos. Todos por el mero hecho de ser ciudadanos tenemos un derecho a ser aislados de los intereses estatales sobre nosotros, pero debemos actualizarlos. Así, la potencia del derecho se comprueba en la propia carta de derechos. Aunque ni la Constitución Federal de 1787 ni sus Enmiendas reconocen expresamente un «*right to privacy*», su Cuarta Enmienda limita la intrusión del gobierno en las personas, domicilios, documentos y efectos personales, incluyéndose no sólo los supuestos de invasión material (*physical trespass*) sino también de vigilancia electrónica frente a registros y requisas arbitrarias (*unreasonable searches and seizures*). No obstante, el derecho a la privacidad en Europa es mucho más estricto que en Estados Unidos.

Hasta el 2015, existía un acuerdo EEUU-Europa llamado *Safe Harbor* que permitía la transferencia de datos entre ambas partes. En 2015, la filtración masiva de datos por parte de Edward Snowden permitió a los Estados conocer las actividades de vigilancia masiva de EE. UU. (similar a la China pero subrepticia) y una demanda de un activista austriaco desembocaron en un fallo de la Corte Europea de Justicia que anuló el acuerdo de *Safe Harbor* por considerar que los estándares de protección de datos de los Estados Unidos no cumplían con los requisitos europeos. En 2016, se adoptó un nuevo acuerdo: el *Privacy Shield*. Este acuerdo incluye elementos de protección más féreos. Como bien señala el Profesor Morales en su discurso de entrada en esta misma academia el 11s “desencadena la lógica de la seguridad; los Estados se encaminan a una cruzada contra la misma, los ordenamientos jurídicos, poco a poco, van a quedar contaminados por las reglas de la lucha contra el terrorismo organizado. Se trata de organizar los instrumentos jurídicos de la emergencia; lo importante es crear un escaparate de seguridad, de apariencia de respuesta punitiva organizada ante una ciudadanía desconcertada que desconfía de todo y de todos”⁶⁰

⁶⁰ Morales Prats, F. La utopía garantista del Derecho Penal en la nueva “Edad Media”. Real Academia de Doctores.

donde la privacidad decae frente al Estado. El patriotismo es más importante que la propia individualidad del ciudadano.

Lo resume bien el profesor de innovación Enrique Dans: el modelo americano funciona porque existe una aceptación a ciegas que permite que los sistemas informáticos recolecten datos y las “compañías puedan rentabilizar esos datos”⁶¹. Es la lógica del beneficio primitivo en un mercado en el que “todo tiene un precio”, más cuando está exigiendo a Europa que abdique de sus regulaciones proteccionistas sobre la privacidad.

Si China controla abiertamente y Estados Unidos no lo hace, pero facilita que corporaciones tecnológicas lo hagan. ¿Qué sucede en Europa?

El padre Estado europeo

En Europa estamos impregnados por nuestra historia, nuestra cultura y, sobre todo, por la religión. A partir del siglo XVI en Europa la homogeneidad religiosa desaparece y se requiere de nuevos fundamentos del poder. Las guerras religiosas generan la necesidad de un poder soberano capaz de imponer la paz en la colectividad y de apaciguar el protestantismo y el catolicismo. El auge del comercio y el crecimiento de la burguesía enriquecida se rebelan contra el viejo derecho estamental y reclaman una igualdad para todos.

La teoría del contrato social europeo justifica su sumisión a las normas sociales buscando la libertad dentro del Estado. Schlaich “pone de relieve el paralelismo entre la doctrina del contrato social y el colegialismo, al mismo tiempo que señala como diferencias entre el Derecho del Estado, derivado del

⁶¹ Dans E, *Viviendo en el futuro*, Planeta, 2019, p.23.

contrato social, y el de la Iglesia, cuyo Derecho está siempre bajo la reserva de la libertad de conciencia, y cuyo poder es el de una simple sociedad, y, por ello, no le está reconocido el *ius imperium*”⁶².

Como bien señala Salome Savona en ‘El Principado’: “a la doctrina del absolutismo regio formulada por Maquiavelo en El Príncipe, y luego apoyada por la Reforma Protestante, se contrapuso en el siglo XVI (1513) la doctrina republicana del “contrato social”. Esta doctrina fue luego respaldada por los jesuitas españoles, como F. Suárez, y los calvinistas franceses o alemanes, como J. Althusius, que defenderán el principio de la Soberanía popular, es decir el origen ético-jurídico del poder político, o el estado de derecho, frente a la Teocracia”⁶³. Los europeos asumimos al padre Estado casi como el Padre Espiritual y, por eso, le dejamos que nos regule.

Nuestro contrato social nos protege frente al Estado absolutista (en idéntico sentido que el americano) y frente a las tecnológicas obligándonos a mantenernos informados sobre la recopilación de nuestros datos e impidiendo, con mayor o menor fortuna, que se comercialice con los mismos. En Europa no nos dejamos controlar salvo para que el Estado nos proteja. En Europa nuestro contrato social se ha modificado poco desde el diseñado por Rousseau. En Europa exigimos sin ceder derechos algo que, como se verá, es (y ha sido) materialmente imposible.

⁶² Die Kirche als Anstalt, citado en Roca, MJ, La influencia de la reforma protestante en el derecho, e-Legal History Review, 2012 (14). pp. 1-35.

⁶³ Salamone, MA, Desde el republicanismo clásico hasta el contractualismo moderno: el De Principatu de M. Salamone y el Principatus Politicus de F. Suárez, Ingenium: Revista electrónica de pensamiento moderno y metodología en historia de las ideas, N.º. 5, 2011, págs. 189-207

Hacia un contrato social digital humanista basado en la confianza

Los monopolios tecnológicos “han obstaculizado la innovación y generado condiciones poco competitivas en determinados mercados”⁶⁴. Y este aspecto es importante porque como señala la doctrina: “Una entidad privada que controle amplias reservas de datos personales posee un poder predictivo que le permite tener una participación desigual en el sistema compartido. Ahora es bien sabido que Google, por ejemplo, tiene suficiente dominio de los datos para predecir las tendencias del mercado de valores con un alto grado de exactitud. Agentes de la compañía han afirmado que dejaron de hacerlo cuando determinaron que sus acciones podrían ser ilegales”⁶⁵.

El miedo se transforma en odio y es, por eso, que debemos cuanto antes articular un nuevo contrato social. El avance de los populismos y nacionalismos es un problema real que en España conocemos bien. Los discursos a favor de los derechos humanos y de la igualdad quedan soterrados frente a la propaganda del odio. Adorno⁶⁶, tras un estudio del resurgimiento del fascismo, propone que frente a ellos hay que utilizar la fuerza “de la razón”, sin ideologías. Sin embargo, su propia ideología neomarxista empaña su discurso que se entiende solo con una lectura pausada del pensamiento del “capitalismo progresista” que representa el Premio Nóbel Joseph Stiglitz. “Las naciones se enriquecen —y alcanzan una mayor calidad de vida— haciéndose más productivas, y la fuente más importante de aumentos en la productividad es fruto de los aumentos en el conocimiento. Los

⁶⁴ Nielsen, M, Who Owns Big Data?, recuperado en Big Data: ¿a quién pertenece? | OpenMind (bbvaopenmind.com)

⁶⁵ Al-Rodhan, N, op. cit.

⁶⁶ Adorno, T. W., y Horkheimer, M. La sociedad. Lecciones de sociología. Trads. Floreal Mazía e Irene Cousien. Proteo, 1971.

progresos tecnológicos dependen de fundaciones científicas financiadas con fondos gubernamentales para la investigación básica. Y las naciones se enriquecen como consecuencia de una buena organización general de la sociedad, que permita al pueblo interactuar, comerciar e invertir con seguridad. El diseño de una buena organización social es el producto de varias décadas de razonamiento y deliberación, observaciones empíricas de lo que ha funcionado y lo que no. Ello ha conducido a conclusiones sobre la importancia de las democracias donde imperan el derecho, el debido proceso legal, los sistemas de pesos y contrapesos y una mirada de instituciones implicadas en descubrir, evaluar y decir la verdad”⁶⁷.

Es cierto una sociedad menos dividida, una economía con mayor equidad, funciona mejor. Por ello el acceso a internet debe ser universal y gratuito. Si se reduce la desigualdad se reduce el miedo y el odio. Se debe buscar una prosperidad compartida que hoy se puede llegar a conseguir gracias a los datos y a los avances tecnológicos, evitando el monopolismo de las empresas que controlan nuestra nueva personalidad digital. Y quiero acabar con las palabras del Stiglitz: “aunque Trump y los nativistas de todo el mundo busquen culpar a otros —los inmigrantes y los malos acuerdos comerciales— de nuestros apuros, y especialmente los de quienes sufren a causa de la desindustrialización, la culpa la tenemos nosotros: podríamos haber gestionado mejor la globalización y el proceso de cambio tecnológico, de manera que al perder su empleo la mayoría de los individuos obtuviera uno nuevo en otro frente. Para seguir adelante, deberemos hacerlo mejor y lo que busco es describir cómo puede hacerse. Lo más importante, con todo, es que el aislacionismo no es una opción. Vivimos en un mundo muy interconectado y, por tanto, debemos gestionar nuestras rela-

⁶⁷ Stiglitz J, *Capitalismo progresista: La respuesta a la era del malestar*, op. cit. p.27.

ciones internacionales —tanto económicas como políticas— mejor que en el pasado”⁶⁸.

Existe ya un “Manifiesto por un nuevo pacto digital”, elaborado por Telefónica donde se indica que “la revolución digital precisa un marco renovado de valores y una modernización de políticas. Necesitamos una Carta de Derechos Digitales mientras las empresas deben asumir la responsabilidad del impacto de la tecnología en nuestras vidas”⁶⁹.

El nuevo contrato social de la humanidad

Convenir un contrato social para toda la humanidad analógica es más que improbable salvo que centremos un contrato con especificidades por territorio. Por ello, debemos centrarnos en tener un contrato social para la persona digital que sea único en todo el mundo y en el que la persona sea el centro y se base en los siguientes puntos⁷⁰:

- Que el proceso de digitalización no deje nadie atrás.
- Modernización de las instituciones y las políticas sociales y culturales.
- Una nueva “Carta de Derechos Digitales” que proteja nuestros derechos fundamentales de la nueva persona digital.
- Compromiso en innovación y emprendimiento.
- Un acuerdo colectivo sobre cómo asegurar la sostenibilidad de la digitalización a base de mejorar la inclusividad, la transparencia y la capacidad de elección, la rendición de cuentas, la responsabilidad y la equidad y no discriminación.
- La devolución de los datos personales a la persona que gestionará su derecho de acceso.

⁶⁸ Stiglitz J, op. cit. p.59

⁶⁹ Tornero, D, op. cit.

⁷⁰ Un nuevo Pacto Digital (telefonica.com)

Y, todo lo anterior, sustentado en el punto más importante: un acuerdo colectivo fundamentado en la confianza en las empresas tecnológicas que nos facilitan el acceso a internet, en las empresas que nos permiten navegar y en los Estados que regulan nuestra personalidad digital. Porque la confianza es lo que permite que otorguemos nuestro consentimiento limitado y compartimentado a cada una de las empresas e instituciones que necesitamos para completar nuestros derechos como personas digitales.

Los ciudadanos empiezan a desconfiar de las empresas de datos y los sistemas para anonimizar nuestros rastros digitales aumentan. Bill Clinton dijo en una ocasión: “No hay nada negativo en Estados Unidos que no pueda curarse con lo que hay positivo en Estados Unidos”. Pues bien, algo así sucede con los datos. Serán nuestra cura, la medicina que necesitamos para creer sin interrupciones. Los datos nos permitirán evolucionar de forma vertiginosa con una red de sujeción: nuestro cerebro que mantendrá la evolución de las nuevas tecnologías en su sitio. Somos más eficaces que las máquinas.

El contrato social, en el contexto de la comunicación en línea, es un contrato hipotético que las personas sienten que tienen cuando comparten sus informaciones personales con las empresas en línea nadie las conoce. Basado en la teoría del contrato social (Fogel y Nehmad)⁷¹ se argumenta que cuando las personas confían en una empresa para que utilice su información personal de forma segura (contrato social confiable) es más probable que comparta sus datos. Si no se les asegura la confianza no cederán sus datos y buscarán medidas de protección para poder seguir navegando, aunque sea más lento, para poder

⁷¹ Fogel, J., & Nehmad, E, Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25 (1), p. 153–160

sentirse seguros. Si se sienten inseguras tenderán a no compartir sus datos (tragedia de los comunes) y eso provocará que actividades como la medicina se vean mermadas de recursos (bienes públicos).

Históricamente el Contrato Social se estudia “con Grotius, Hobbes, Locke y, por supuesto, Rousseau, quienes exploraron los límites de la libertad individual y el poder de la soberanía. Desde el concepto de estado como “juez neutral” de Locke, hasta Rousseau, Rawls y otros, todas las perspectivas del contrato social buscan en último término analizar por qué los individuos racionales aceptarían renunciar a algunas de sus libertades como contrapartida de vivir en un orden político”⁷². En la era nueva es el contrato que mantenemos con las empresas de gestión de datos a la que exigimos confianza y que no traspasen el límite impuesto para el uso de estos. Es por ello por lo que la confianza es la base del contrato social. Volvemos al concepto de nuestros antiguos, en que darse la mano era más importante que firmar un contrato. Confiar es la única forma de evolucionar en el mundo actual. Pero esa confianza ahora lleva aparejada un contrato y unas sanciones por incumplirlo.

En suma, tanto el riesgo como la confianza (es decir, la dimensión de riesgo de confianza) juegan un papel fundamental en la predicción de diferentes comportamientos relacionados con la privacidad⁷³. Para Al-Rodhan “la tecnología podría alterar las condiciones de un contrato social, la capacidad de mejora individual por medios tecnológicos sugiere que ya no están garan-

⁷² Al-Rodhan, N, Geneva Centre for Security Policy. Ginebra, Suiza publicado en Harvard International Review, The Social Contract 2.0 Big Data and the Need to Guarantee Privacy and Civil Liberties Politics in Spires, traducido en El contrato social 2.0: Big Data y la necesidad de garantizar la privacidad y las libertades civiles | OpenMind (bbvaopenmind.com)

⁷³ Blanco, F y Blasco G, Un análisis de la influencia de la confianza y el riesgo percibido sobre la lealtad de un sitio web: el caso de distribución de servicios gratuitos, en Revista Europea de Dirección y Economía de la Empresa, vol. 16, nº 1, 2000, pp. 159-178.

tizados los tipos fundamentales de igualdad que los primeros teóricos del contrato social fueron capaces de presuponer. “Para Hobbes y los herederos de su tradición, la relativa igualdad de fuerzas garantizaba la vulnerabilidad universal de todo. Un radical aumento de la habilidad mental y física de ciertos individuos gracias a la biotecnología y la biología sintética invalidaría la presunción de vulnerabilidad compartida y, con ello, la base fundamental de la posibilidad de un contrato social. Aunque el potencial de la tecnología para obtener tales resultados es real y significativo, otras manifestaciones son mucho más avanzadas, y ya han generado efectos palpables en las relaciones intraestatales e interestatales”⁷⁴⁷⁵.



⁷⁴ El contrato social 2.0: Big Data y la necesidad de garantizar la privacidad y las libertades civiles recuperado en El contrato social 2.0: Big Data y la necesidad de garantizar la privacidad y las libertades civiles | OpenMind (bbvaopenmind.com)

⁷⁵ Al-Rodhan, N, Geneva Centre for Security Policy. Ginebra, Suiza publicado en Harvard International Review, The Social Contract 2.0 Big Data and the Need to Guarantee Privacy and Civil Liberties Politics in Spires, op. cit.

❖ CAPÍTULO 4. EL POPULISMO ROBÓTI- CO, LA EDUCACIÓN Y EL *BIG DATA*

España debate en la actualidad sobre si en su sistema educativo cabe (o no) la memorización. La nueva ley de educación pretende sustituir el modelo enciclopédico por otro basado en la aplicación y relación de los conocimientos. El ataque proviene de aquellos que defienden la competencia personal unida a la memoria. Pero España es el paradigma de lo que no se debe hacer en materia de conquista de los derechos en cada revolución industrial. En España rivalizamos contra lo nuevo y no nos damos cuenta de que ya no existe un rival sino el propio futuro contra el que no debemos luchar, si no adaptarnos para descabalgarnos del primer mundo.

Durante la Ilustración, España se quedó atrás aferrada a los miedos atávicos de la religión y a una nobleza que se resistía a dejar su poder. La respuesta al cataclismo español la encontramos en la economía, la historia, la política y la psicología. La Ilustración propició cambios profundos en la Economía con la publicación en 1776 de la obra de Adam Smith, 'La riqueza de las naciones', que se complementaría con otras posteriores de Robert Malthus, David Ricardo y Jean Bautista Say. Sin embargo, algunos se resistieron al cambio. Matt Ridley, autor de 'El optimista nacional', afirma que "lo supersticioso y la burocracia" son el verdadero peligro para el progreso dado que frenan la acumulación de conocimiento e impide la evolución en los negocios⁷⁶ y de miedos atávicos sabemos mucho en nuestro país. Antonio Domínguez Ortiz, académico, y catedrático de Historia señala que "la trayectoria que siguió la Ilustración en

⁷⁶ Ridley M, *El optimista racional: ¿Tiene límites la capacidad de progreso de la especie humana?*, Taurus, 2011.

España no fue una evolución progresiva y homogénea, como en Inglaterra; fue desviada primero por la Revolución francesa, la guerra de la Independencia después y, por último, la radicalización de posiciones políticas en tomo a Fernando VII. Estos factores, unidos a las adversas circunstancias económicas, dificultaron la formación de una burguesía fuerte, que sustentara un régimen político auténticamente liberal, al desaparecer aquel espíritu reformador, aquel término medio que los ilustrados representaban”.⁷⁷

Desde un punto de vista político aparecieron las soluciones rápidas a problemas complejos. El ensayista económico sueco Norberg⁷⁸ señala que los resentimientos y reticencias a la evolución pone de acuerdo a populistas de derechas e izquierdas. “Hay un riesgo real de que estas tensiones alimenten una peligrosa reacción nacionalista. Se ignora el progreso logrado y se buscan chivos expiatorios a quienes endosar los problemas que aún hoy seguimos sufriendo”. La superstición del pueblo y el sesgo religioso impidió entonces que España evolucionase como ocurre hoy con aquellos que se oponen a la globalización.

Por último, los psicólogos Kahneman y Tversky⁷⁹ nos explican por qué los atajos cerebrales nos impidieron llegar a conclusiones certeras poniendo al yo y sus experiencias por encima de lo racional. Atajos mentales que generalmente implican enfocarse en un aspecto de un problema complejo e ignorar otros. Steven

⁷⁷ Entrevista en El País, 25 de abril de 1980.

⁷⁸ Norberg, J, *Progreso: 10 razones para mirar al futuro con optimismo 10 razones para mirar al futuro con optimismo*, Deusto, 2017.

⁷⁹ La teoría prospectiva (Prospect Theory) fue desarrollada en 1979 por los psicólogos Daniel Kahneman (Premio en Ciencias Económicas en memoria de Alfred Nobel en el año 2002) y Amos Tversky. Esta teoría permite describir cómo las personas toman sus decisiones en situaciones donde deben decidir entre alternativas que involucran riesgo. Kahneman, D., y Tversky, A. (1979). Prospect Theory: An analysis of decision under risk. *Econometrica*, 47, 263-292. Kahneman, D., y Tversky, A. (1981). The framing of decisions and the psychology of choice. *Science*, 211, 453-458.

Pinker⁸⁰ desarrolla los sesos psicológicos: lo malo es más fuerte que lo bueno, la moral pretende demostrar al resto nuestras preocupaciones y un tercer sesgo es elogiar el pasado en contra del presente. Y los españoles, si sabemos de algo, es de sesgos, miedos y envidias.

El miedo a las máquinas: máquinas vs humanos

Que una máquina sea mejor que nosotros, genera pesimismo y miedo; es normal. Pero el futuro es así. Los trabajos repetitivos y especializados los harán algoritmos. El humano será el valor añadido. Dejaremos de usar las manos para utilizar el cerebro. ¿Ganaremos la partida de la inteligencia a las máquinas y podremos seguir en la cima de la pirámide? Esa es la pregunta que me hice cuando entendí que el mundo pasaba por transformarse digitalmente. La respuesta la dio Garry Kasparov, uno de los mejores jugadores de ajedrez de la historia en una de sus conferencias. Al escucharlo entendí por qué debemos cambiar aquel sistema educativo en el que nos enseñaban a saber y no a comprender.

“Esta historia empieza cuando a los 22 años gané el Campeonato Mundial de Ajedrez tras vencer a Anatoli Kárpov”⁸¹. Estas fueron las primeras palabras que pronunció en una de las conferencias que dio en nuestro país. Se remonta a 1985, y recuerda que entonces también estuvo en Alemania jugando partidas simultáneas contra treinta y dos de las mejores máquinas de ajedrez del mundo. “Fue mi edad de oro”, recuerda. Pero doce años después algo cambió. Jugó dos partidas memorables contra la supercomputadora Deep Blue de IBM en 1997. Y, después de sudar la gota gorda, perdió la segunda. En el enfrentamiento del ser humano contra el ordenador, la máquina le

⁸⁰ Pinker, S. *En defensa de la Ilustración*, op. cit.

⁸¹ Sanz, E., *El mensaje de Kasparov sobre las máquinas inteligentes*, Heraldo de Aragón, 2017.

había ganado al cerebro, decían los titulares. Eric Brynjolfsson y Andrew McAfee explican una anécdota sobre cómo derrotar a las máquinas, en su libro ‘La segunda era de las máquinas’⁸². Le preguntaron al maestro de ajedrez Donner cómo prepararía una partida contra Deep Blue y contestó: “llevaría un martillo”. Pero la realidad es que las máquinas ganarían la partida si tuviesen emociones, algo que no ocurrirá.

El sistema educativo se ha basado en la acumulación de datos y su memorización. Hoy cualquier máquina, por pequeña que sea, lo hace mejor que los humanos. Libratus, un *bot* con inteligencia artificial diseñado por un profesor de ciencias y uno de sus estudiantes de doctorado, ganó a cuatro de los mejores jugadores de póquer del mundo en un torneo de veinte días de Texas Hold’Em en 2017. Las probabilidades de que Libratus ganara eran de 4 a 1 y su éxito fue tal que se aceptó un trabajo jugando a juegos de guerra para el Pentágono.⁸³ La prueba de acceso de una Universidad de Tokio la hizo mejor un robot que el 80% de los alumnos⁸⁴. Los investigadores de DeepMind, la filial de inteligencia artificial de Google, han conseguido que sus jugadores electrónicos sean capaces de jugar y ganar a un videojuego multijugador en línea, algo imposible hasta la fecha, y que implica cooperar y competir con otros jugadores.

¿Para qué memorizar entonces? Nuestro cerebro está por descubrir. La UE y los Estados Unidos han puesto en marcha dos proyectos: *Humann Brain Project* y *Brain*, respectivamente, para descubrir todas las habilidades de nuestro cerebro. Los investigadores del Grupo Redes de Neuronas Artificiales señalan que los parecidos entre el cerebro y el ordenador se reducen a que

⁸² McAfee, A., La segunda era de las máquinas, Temas, 2013, p. 10.

⁸³ <https://blog.betway.es/casino/el-ser-humano-contra-la-maquina-qui-en-se-impondra-1/>

⁸⁴ <https://elfuturoesapasionante.elpais.com/robot-capaz-aprobar-las-pruebas-acceso-la-universidad/>

ambos utilizan el almacenamiento y procesamiento de información y para ejecutar tareas. Ya está. El resto es diferente y en muchos casos salimos perdiendo: los ordenadores son mucho más rápidos y eficientes. Pero el cerebro es creativo, interpreta los sentidos y analiza de forma innovadora. En este sentido, uno de los mayores especialistas en Inteligencia Artificial (IA) de nuestro país, el doctor Pablo Rodríguez, señala que: “el número de transistores de un ordenador cada vez se acerca más al número de neuronas de un cerebro humano, aunque el cerebro gana en cuanto a número de conexiones”⁸⁵. El cerebro usa reglas y algoritmos para hacer predicciones, se perfecciona y evoluciona, como los ordenadores. Incluso, se habla, de “interpolinización” entre ordenadores y cerebros, o de cerebros electrónicos o de computadoras cerebrales. Sea lo que sea no podemos obviar que de un ordenador ya se conoce todo y en un cerebro ni un 10% se conoce. La Inteligencia Artificial pretenderá simular nuestro cerebro, no al revés. Y mejorarán en casos, pero nunca aprenderán a socializar. No tendrán contrato social. Por eso ganaremos la partida a las máquinas. Las usaremos para que hagan todo lo que no queremos hacer y sea reiterativo. Dejaremos de ser esclavos del trabajo. Sea como fuere la clave está en la comunicación y en la socialización, es decir, en la base del contrato social.

A pesar de la afirmación previa, se calcula que hasta una quinta parte de la población activa mundial podría perder su trabajo en 2030 por la automatización basada en robots. Google ya ha dado a un sistema llamado *Duplex*, que entabla «conversaciones sofisticadas» y completa tareas administrativas, como concertar citas. Los robots se están adentrando incluso en los sectores creativos. Unos 850 artículos de la cobertura electoral estadounidense del *The Washington Post* en 2016 fueron escritos por un programa robot de noticias llamado *Heliograf*. Pero

⁸⁵ Rodríguez, P. *Inteligencia Artificial: cómo cambiará el mundo (y tu vida)*, Deusto, 2018.

tanto Google, como Facebook o Uber prevén que solo hay un 50 % de posibilidades de que los robots asuman todos los trabajos de los humanos en 120 años. Un robot puede realizar tareas en un laboratorio, pero manipularlos para que trabajen en el mundo real no es tan sencillo. Se necesita cerebro. Un robot puede imitar una conversación natural, pero nunca podrá tener emociones propias de la socialización. Un informe del Foro Económico Mundial defiende que las IA podrían generar 133 millones de puestos de trabajo en 2022 al liberar a los trabajadores para que hagan nuevas tareas. Los robots son más eficientes, pero no más eficaces.

Según la Real Academia de la Lengua Española, eficacia se refiere a la “capacidad de lograr el efecto que se desea o se espera”, mientras que eficiencia es definida por este organismo como la “capacidad de disponer de alguien o de algo para conseguir un efecto determinado”. Desde un punto de vista empresarial, una persona eficaz es aquella que consigue cumplir con un objetivo en el tiempo señalado; en cambio, será eficiente si alcanza la meta empleando los menos recursos posibles. Kilian Zambrano en su obra *Planificación y control de la producción pública*⁸⁶, señala dos conceptos:

- Principio de eficacia: «La obtención de los resultados deberá exigir la menor cantidad de eventos posibles. El encuentro y la fricción deberán minimizarse y solo producirse como eventos encadenados integral y orgánicamente orientados hacia los resultados».
- Principio de eficiencia: «El actor estratégico hará un uso dosificado de sus recursos en cada evento del juego interactivo, lo cual ocurrirá en función de la aplicación de recursos por parte del otro”.

⁸⁶ Zambrano, K., *Planificación y control de la producción pública*, recuperado en servicio.bc.uc.edu.ve

La propia Constitución Española exige, en su artículo 103, a la Administración Pública eficacia: “La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho”. En realidad, debería exigir eficacia y eficiencia si quiere que los ciudadanos estén contentos con el servicio público. Pero en la vida la eficiencia solo se consigue sociabilizando. Amazon analiza a sus empleados con *Anytime Feedback Tool*. La empresa americana tiene claro que el cliente es el centro de valor y analiza a sus empleados para acortar el tiempo entre que el producto sale de sus centros logísticos y llega a nuestras casas. Sabe qué empleado está más cerca del producto, le indica el camino para que lo recoge y lo ponga en el sistema de envíos. Todo por el cliente. Luego si el producto no gusta nos permite devolverlo sin más; ahí gana Amazon por su eficiencia, a pesar de que el producto que nos llegue no sea eficaz. La eficacia sólo se consigue escuchando y ofertando. La eficacia solo la puede dar el cerebro. La eficacia la da el lenguaje y es el lenguaje el que nos hace estar en la pirámide de los datos.

La memorización, por tanto, será para las máquinas y la inteligencia de los datos memorizados la debe aportar el hombre que se convertirá en la cadena de valor de este mundo interrelacionado que llega. Pero el problema será en cómo nos relacionamos con los robots.

Personalidad jurídica de los robots

Un informe de la Comisión de Asuntos Jurídicos del Parlamento Europeo de enero de 2017 reconoce que las mejoras en las capacidades autónomas y cognitivas de los robots las convierten en algo más que simples herramientas y que las “normas ordinarias sobre responsabilidad, como la responsabili-

dad contractual y la responsabilidad extracontractual, son insuficientes para manejarlas”⁸⁷. Se abrió entonces una discusión sobre la necesidad de otorgar (o no) personalidad jurídica a los robots.

Los partidarios de otorgarla abogan por considerar a los robots como personas electrónicas⁸⁸ instaurando una responsabilidad objetiva por daños y una carta de derechos y obligaciones⁸⁹. Quintero Olivares sostiene que se podría establecer una “personalidad de los autómatas”, pero como una personalidad diferente, que, en el fondo, tomaría ese nombre por analogía. Añade que “tampoco sería escandaloso que se hablara de la “personalidad” de los robots como objeto de unas normas legales”⁹⁰. Sin embargo, si consideramos que el robot es una mera máquina, tendría entonces el estatus jurídico de cosa, siendo el diseñador y el programador, su responsable jurídico. Desde el punto de vista jurídico las cosas son consideradas objetos materiales, muebles o inmuebles (art. 333 Código Civil). Otra cuestión es la de crear una ficción jurídica, como señala parte de la doctrina⁹¹, y equiparar al robot a la persona jurídica.

En este sentido, dos centenares de expertos de catorce países europeos, en una carta abierta dirigida al presidente de la Comisión Europea, Jean-Claude Juncker, manifestaron su rechazo a la “personalidad electrónica” que el Parlamento Europeo en la Resolución, de 16 de febrero de 2017, pretendía otorgar a los

⁸⁷ Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (europa.eu)

⁸⁸ Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, p. 17.

⁸⁹ Puyol, J., “Robots: ¿Hacia un nuevo concepto de “personalidad jurídica?””, 2018. Disponible en: <https://confi legal.com/>

⁹⁰ Quintero Olivares, G., “La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas”, *Revista Electrónica de Estudios Penales y de la Seguridad*, nº 1, 2017, p. 7.

⁹¹ Por todos, Santos González, MJ., “Regulación legal de la robótica y la inteligencia artificial: retos de futuro”, *Revista jurídica de la Universidad de León*, nº 4, 2017, p. 27

robots. En idéntico sentido, Griseri señala que otorgar derechos a un robot es una “idea peligrosa”⁹² y añade: “El Comité de Asuntos Jurídicos de la Unión Europea está caminando a ciegas en un pantano si piensa que la personalidad electrónica protegerá a la sociedad de la evolución de la Inteligencia Artificial. La analogía con la personalidad jurídica es desafortunada, ya que esto no ha protegido a la sociedad en general, sino que ha permitido a los propietarios de empresas promover sus propios intereses”.

Sin entrar en todo el debate que se estableció se debe declarar *tot court* que, si reconocemos una “personalidad jurídica electrónica”, como ha propuesto el Parlamento Europeo, se les debería otorgar “derechos y obligaciones”, algo consustancialmente absurdo porque las cosas pueden tener obligaciones, pero no derechos. Un “reconocimiento jurídico de su subjetividad, fundamentalmente en derechos de naturaleza patrimonial, pero no los constitucionales ni los de la personalidad, absolutamente consustanciales a la dignidad de los seres humanos”⁹³. Por tanto, como se señala en las propuestas *lege ferenda* de Barros, cualquier “regulación debe preservar valores como la autenticidad, seguridad y protección de la raza humana, regular las cuestiones éticas y los conflictos que puedan surgir en las relaciones robot persona y entre robots. No se trata de regular la tecnología sino de regular la sociedad para que siga siendo para los humanos como ellos decidan”⁹⁴.

⁹² Griseri, P, “Giving rights to robots is a dangerous idea”, 2017 recuperado en <https://www.theguardian.com/technology/2017/jan/16/giving-rights-to-robots-is-a-dangerous-idea>

⁹³ Véase el brillante trabajo de grado de Laura Barros, El debate sobre la personalidad jurídica y la responsabilidad de los robots inteligentes. Especial referencia a la robótica sanitaria, recuperado en el debate sobre la personalidad jurídica y responsabilidad de los robots inteligentes. especial referencia a robótica sanitaria (unican.es)

⁹⁴ Barros L, op. Cit.

La cadena de valor: el hombre en la quinta revolución industrial

Los futurólogos anuncian un mundo robotizado donde los coches serán autónomos, nuestro smartphone controlará nuestra casa y donde las tiendas físicas dejarán de existir. Todo ello supone un rastro de datos. Las aplicaciones nos regalan producto a cambio de nuestra opinión (nuestros datos). Si queremos acceder a contenido deberemos dar nuestra identificación. El *Big Data* está presente e integrado en nuestro día a día, sin que nos demos cuenta de ello.

El término *Big Data* por primera vez en los años 90 gracias a un artículo publicado por el estadounidense John Mashley, un reconocido informático teórico (*Big Data and the Next Wave of Infrastrass*)⁹⁵. En el estudio explicaba cómo iban a cambiar los procesos de trabajo, las herramientas y técnicas empleadas para el análisis de datos en el mundo de la informática. Mashley anticipó los aspectos sobre la forma en que entenderíamos y podríamos aprovechar la inmensa cantidad de datos que se generarían en el futuro. Los datos son el nuevo petróleo, el combustible con el que las empresas harán negocio (ya lo hacen) en el futuro. Los riesgos asociados a los datos son: la discriminación predictiva en el sector de la medicina, empleo y seguros; la pérdida del anonimato; el control gubernamental; el negocio de la compraventa de datos; los riesgos de la seguridad. Los bancos ya no guardan dinero, controlan flujos de pagos. Las empresas como Mytaxi (ahora Freenow) ya no venden servicios de taxi sino los datos que obtiene en tiempo real del uso de vehículos de uso por tiempo reducido. Por eso la compró Daimler. Los fabricantes de coches saben que “en breve dejarán de vender coches para pasar a ofrecer servicios de

⁹⁵ Mashley, J., recuperado en [/var/tmp/biggest.data.ps \(usenix.org\)](#)

movilidad”⁹⁶. En poco tiempo ya nadie comprará coches, los compartiremos. La tecnología ya es una innovación aceptada por todos. Hemos asumido que el cambio está aquí y que es irremediable. Estamos en una época disruptiva, lo sé. Pero los taxistas deberán adaptarse, igual que lo hizo Correos cuando apareció el correo electrónico.

El coche eléctrico se inventó en 1990. Veinte años atrás, Thomas Edison, las baterías recargables, pero no ha sido hasta ahora que lo hemos aceptado. Tesla es tecnología. No vende coches, sino baterías. HP vende tinta, no impresoras. Brita vende filtros de agua, no jarras. Los detectives no venden datos, sino inteligencia de datos. Y todo porque la cadena de valor se ha trasladado desde la “ventaja competitiva” identificada por Michael Porter⁹⁷ en 1985, hacia el cliente. Él (nosotros) lo es todo. Es el centro del mundo. Por eso los servicios donde el cliente no sea el centro de la cadena de valor desaparecerán. En eso, tampoco, los robots nos superarán. El rival ya no es otra empresa, tampoco los robots, el rival es el propio futuro. O nos adaptamos o seremos analfabetos funcionales en paro. Primero llegaron los robots, luego la inteligencia artificial. La evolución sólo se consiguió con la unión de ambas disciplinas. Los datos han sido el pegamento que ha permitido la transformación digital. Déjenme explicarme. La era de los robots ha llegado para quedarse, pero ha tardado. En 1954, el inventor George C. Devol patentó un diseño para un brazo mecánico programable. En 1961, el empresario Joseph Engelberger convirtió ese diseño en Unimate, una máquina que se utilizó por primera vez en una línea de montaje de General Motors, y que se convertiría en el primer robot de la historia,

⁹⁶ Vidal, M., *La era de la humanidad: hacia la quinta revolución industrial*, Deusto, 2019.

⁹⁷ Porter, M., *Ventaja competitiva: creación y sostenimiento de un desempeño superior*, Grupo Patria Cultural, 2002.

según la revista MIT Technology⁹⁸. Entonces y ahora eran máquinas dirigidas a realizar tareas específicas con un software muy simple.

La inteligencia artificial siguió un camino diferente, señala la misma revista. “En la década de 1950, se propuso la idea utilizar la informática para imitar la lógica y la razón humana. Algunos investigadores también querían dar a estos sistemas una presencia física. En 1948 y 1949, el neurocientífico en Bristol (Reino Unido) William Gray Walter, desarrolló dos pequeñas máquinas autónomas a las que denominó Elsie y Elmer. Estos dispositivos, con un diseño parecido a una tortuga, estaban equipados con circuitos simples inspirados en la neurología que les permitían seguir una fuente de luz por sí mismos. Walter los construyó para demostrar que un pequeño número de conexiones neuronales da lugar a un comportamiento relativamente complejo”⁹⁹.

Y todo se estancó hasta que hace pocos años Geoffrey Hinton descubre el *Deep learning* (aprendizaje profundo): “El avance de Hinton, en 1986, fue demostrar que la retropropagación servía para entrenar una red neuronal profunda, es decir una con más de dos o tres capas. Pero fue necesario que pasaran otros veintiséis años antes de que el aumento del poder computacional diera por bueno el descubrimiento. Un artículo publicado en 2012 por Hinton y dos de sus estudiantes de Toronto (uno de ellos ganador de Innovadores menores de 35 globales en 2015) demostró que las redes neuronales profundas, entrenadas con retropropagación, superaban a los sistemas más avanzados de reconocimiento de imágenes. El “aprendizaje profundo” despegó. Para el mundo exterior, la IA parecía des-

⁹⁸ Recuperado en <https://www.technologyreview.es/s/10340/el-alzamiento-de-los-robots-por-fin-ha-llegado-gracias-la-ia>

⁹⁹ Op. cit.

pertar de la noche a la mañana. Para Hinton, era una recompensa largamente merecida”¹⁰⁰.

Ahora gracias a una cámara y un software de aprendizaje automático ejecutado en un ordenador, el robot descubre cómo ser más eficaz. “Al colocar un software de IA en un cuerpo físico, la máquina se vuelve capaz de identificar objetos, comunicarse y navegar por el mundo real. Y la inteligencia artificial se vuelve más potente cuantos más datos consume. Así que cada vez que el robot lleva a cabo una tarea, el software que actúa como cerebro va adquiriendo más conocimientos sobre el mundo y cómo funciona”¹⁰¹. Esto podría dar lugar a avances que “sin todos esos datos serían imposibles”, afirma el profesor de la Universidad de California en Berkeley Pieter Abbeel¹⁰². Y a pesar de ello el pesimismo reina en los científicos. Un nubarrón se acerca a nosotros: la pérdida de los derechos y, peor aún, como señala el nobel Joseph Stiglitz una amenaza para la democracia¹⁰³.

La quinta revolución industrial

Transitamos la cuarta revolución industrial y debemos hacerlo con la mirada puesta en la quinta. Marc Vidal, una de las figuras más influyentes en la transformación digital señala en su libro ‘La era de la humanidad’ que la “hipertransformación del todo que nos espera en muy pocos años culminará con lo que

¹⁰⁰ <https://www.technologyreview.es/s/9600/el-hallazgo-de-hace-30-anos-en-el-que-se-basa-toda-la-inteligencia-artificial-actual>

¹⁰¹ <https://www.technologyreview.es/s/10340/el-alzamiento-de-los-robots-por-fin-ha-llegado-gracias-la-ia>

¹⁰² Citado en Inconday, Entrenando a Robots como Títeres en el que se señala que: “esa es la visión de Pieter Abbeel, profesor de ingeniería eléctrica y ciencias de la computación en la Universidad de California, Berkeley, y sus estudiantes, Peter Chen, Rocky Duan y Tianhao Zhang, que han lanzado una startup, Embodied Intelligence Inc., para usar el las últimas técnicas de aprendizaje de refuerzo profundo e inteligencia artificial para hacer que los robots industriales sean fácilmente enseñables”

¹⁰³ Stiglitz, J. Capitalismo progresista, op. cit. 140.

se ha llamado la singularidad tecnológica”¹⁰⁴. En un futuro cercano los ordenadores tendrán funciones propias del cerebro humano que se mejorarán a sí mismas. Nos dirigimos, según el autor, a un “escenario caracterizado por el mundo automatizado (robótica), cognitivo (inteligencia artificial) y de acceso inmediato a los datos. Está por venir el internet del todo. Todo estará conectado y será medible con el *big data*”¹⁰⁵.

La expresión “revolución industrial 4.0” proviene del foro de Davos de 2016. Durante la tradicional rueda de prensa que antecede cada año a la reunión anual en Davos, el fundador del Foro Económico Mundial, el profesor de la Universidad de Ginebra Klaus Schwab¹⁰⁶, hizo un llamamiento a los líderes mundiales a que revisen sus políticas para adaptarlas a los cambios que se avecinan. “Aún no estamos suficientemente preparados para esta cuarta revolución industrial y temo que llegará como un tsunami y transformará todos los sistemas y procesos”, dijo. La falta de preparación golpeará aún más a la clase media e “incrementará los problemas de exclusión social que vive el mundo, algo que debemos evitar a toda costa”, añadió.

Los factores que impulsaron la cuarta revolución industrial son: los cambios en los entornos de trabajo y las jornadas laborales flexibles, el aumento de la clase media en los países emergentes, el cambio climático, la restricción de los recursos naturales, la transición a una economía más verde, el aumento de la volatilidad política, la población joven de los mercados emergentes y la rápida urbanización se consideran factores del cambio cuyo impacto ya se ha sentido en el orden mundial. Ya en 2016 se anunció la quinta revolución industrial: “el Internet

¹⁰⁴ Vidal, M., *La era de la humanidad: hacia la quinta revolución industrial*, op. cit.

¹⁰⁵ Vidal, M., op. cit.

¹⁰⁶ Pérez, MJ. Davos y la cuarta revolución industrial, recuperado en Davos y la cuarta revolución industrial (unir.net)

móvil y la tecnología en la nube, los avances en informática y en Big Data (análisis de grandes cantidades de información), las nuevas fuentes de energía y tecnologías, el Internet de las cosas (es decir, la presencia de Internet en prácticamente todo aquello que utilizamos en nuestro día a día), los avances en robótica y en el transporte autónomo, la inteligencia artificial, la fabricación avanzada y la impresión en 3D y, por último, los materiales, la biotecnología y la genética avanzada”¹⁰⁷.

Políticos y economistas discuten sobre cómo afrontar el futuro mientras nuestros gobernantes miran hacia otro lado y se aumentan los impuestos a las empresas tecnológicas simplemente por serlo. El nobel Joseph Stiglitz señala que “si la innovación no se gestiona bien, en lugar de traer prosperidad a todos, podría tener el efecto opuesto”¹⁰⁸. Irlanda, al contrario que España, fomenta un sistema impositivo favorable a las empresas con un impuesto de sociedades, del 12,5%. “Esta tasa impositiva no solo facilita los comienzos a las nuevas empresas, también es un factor de atracción para las grandes tecnológicas y ha sido una sustancial fuente de polémica en Bruselas”¹⁰⁹. Dublín acoge las sedes de Facebook, Google, Microsoft, Paypal, eBay o Intel. Este régimen fiscal, que también practican otros miembros de la UE como Luxemburgo o Países Bajos, se orienta a atraer capital y estimular la economía local. Un análisis de la compañía financiera Funderbeam apunta que hay 34 compañías emergentes por cada 100.000 habitantes en el país, la segunda mayor proporción tras la de Islandia. En 2018 se invirtieron 930 millones de euros en 223 startups irlandesas, según la asociación TechIreland. En un informe específico, autoridades de exportación del Ministerio de Economía de Países Bajos

¹⁰⁷ Pérez, MJ, op. cit.

¹⁰⁸ Stiglitz, J, Capitalismo progresista, op. cit.

¹⁰⁹ Recuperado de Irlanda vuelca sus ‘startups’ en la UE ante el Brexit (que no llega) - Hacer Contrato De

hablaban de 2.500 firmas solo en Dublín, 165 centros de desarrollo y aceleradoras y más de 1.200 proyectos empresariales creados en 2017. El Brexit es para los ingleses nuestro derecho a decidir, su cortina de humo. Por eso Irlanda centra su plan de contingencia en la Eurozona.

Un estudio español realizado por la Moncloa este 2021 propone cincuenta objetivos que nuestro país debería alcanzar de aquí a 2050¹¹⁰ defendiendo que la robotización no aumentará el desempleo estructural. Reconoce el informe que la transformación tecnológica provocará la desaparición de muchas ocupaciones y muchos puestos de trabajo reflejando el optimismo de cierta parte de la doctrina¹¹¹ en cuanto a la creación de nuevos puestos al calor de las transformaciones. Y, sin embargo, pierde la oportunidad de crear un marco estructural para debatir sobre los verdaderos problemas del futuro.

El comité de expertos español hace recomendaciones y predicciones para el futuro de España como país y dedica una parte a la fomentar la necesidad de aumentar nuestra productividad y la importancia de la tecnología para lograrlo. El informe centra en nueve los grandes desafíos de nuestro país: “ser más productivos para crecer mejor; conquistar la vanguardia educativa; mejorar la formación y la recualificación de nuestra población; convertirnos en una sociedad neutra en carbono, sostenible y resiliente al cambio climático; preparar nuestro Estado de bienestar para una sociedad más longeva; promover un desarrollo

¹¹⁰ Recuperado en 200521-Estrategia_Espana_2050.pdf (lamoncloa.gob.es)

¹¹¹ Para más detalles véase, David H., y Anna Salomons. “Is Automation Labor-Displacing? Productivity Growth, Employment, and the Labor Share.” *Brookings Papers on Economic Activity*, 2018. <https://doi.org/10.3386/w24871>; Dauth, Wolfgang, et al. “German Robots - The Impact of Industrial Robots on Workers.” *CEPR Discussion Paper*, n.º DP12306, 2017. <https://ssrn.com/abstract=3039031>; Graetz, Georg, y Guy Michaels. “Robots at work”. *The Review of Economics and Statistics*, n.º 5, 2018. https://www.mitpressjournals.org/doi/pdf/10.1162/rest_a_00754; y Nübler, Irmgard. “New technologies: A jobless future or golden age of job creation?” *International Labour Office, Working paper*, n.º 13, 2016. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms_544189.pdf.

territorial equilibrado, justo y sostenible; resolver las deficiencias de nuestro mercado de trabajo y adaptarlo a las nuevas realidades sociales, económicas y tecnológicas; reducir la pobreza y la desigualdad, y reactivar el ascensor social, y ampliar las bases de nuestro bienestar futuro”¹¹².

Pero el Gobierno tira la toalla al reconocer que “es fácil soñar con una España puntera en informática cuántica, Industria 4.0 e Inteligencia Artificial. Sin embargo, la experiencia histórica revela lo difícil que resulta transformar de manera sustancial la estructura productiva de un país en un periodo breve de tiempo, o alcanzar a competidores que llevan décadas invirtiendo en el desarrollo de ciertas tecnologías”.

El futuro está lleno de agoreros.



¹¹² Recuperado en La Moncloa. 20/05/2021. Sánchez presenta ‘España 2050’, un proyecto colectivo para decidir “qué país queremos ser dentro de 30 años” [Presidente/Destacados]

❖ CAPÍTULO 5. EL FUTURO

Lo acabamos de comprobar: España perdió el tren de la Ilustración y no puede permitirse perder el de la revolución tecnológica. El progreso está aquí y la quinta revolución industrial, a pesar de los riesgos y los miedos nos fagocitará. Queramos o no. España puede quedarse, nuevamente atrás o desplazar los atajos mentales, las supersticiones y las luchas políticas. Parece que estemos empeñados en repetir los errores del pasado. Nuestros políticos, aquellos aristócratas contra los que la burguesía (o los nuevos disruptivos) luchó, discuten sobre el pasado mientras otros países como Suecia crean Ministerios del Futuro. Kristina Persson, la primera ministra del Futuro del gobierno de Suecia entre 2014 y 2016 es, además, la directora de un proyecto público para fomentar ideas que afronten los desafíos del futuro llamado *Mission: The Future*¹¹³, indica que es necesario que los políticos adopten medidas urgentes para que el impacto de la inteligencia artificial no arrase a lo que hasta ahora hemos creado.

Persson analiza el futuro en el estudio de cinco aspectos: conocimiento, transformación, gobernabilidad, cooperación y valores. “A medida que el conocimiento siga avanzando y que todos tengan acceso a él, es esencial que los países sigan evolucionando; incluso es una condición para la supervivencia de la raza humana. Segundo, estamos viviendo en un momento de gran transformación de la sociedad y de la economía por el calentamiento global y el desarrollo tecnológico que es tan rápido y disruptivo. Frente a esto, es clave ver cómo se gobierna en este contexto. Y ahí hay que trabajar para desarrollar la habilidad de

¹¹³ Recuperado en *Mission: The Future* - Government.se

que haya cooperación entre países y regiones y también sumar al sector público y académico. Todo esto, sustentado por altos valores morales y éticos”¹¹⁴.

Es un mensaje idéntico al de la Ilustración fijando el foco en nuevos problemas. Nada ha cambiado y todo lo ha hecho. El futuro está aquí y o lo aceptamos o nos arrollará. Quien no se adapte a los cambios tecnológicos, como he dicho y repetiré, será un analfabeto funcional y el tercer mundo no se medirá por sus índices de pobreza sino por sus índices de digitalización. Solo los países que legislen pensando en la nueva revolución industrial se aprovecharán de la nueva era de la humanidad. Stephen Hawking decía que “estamos en el momento más peligroso en el desarrollo de la humanidad” y que el “ascenso de la inteligencia artificial destruirá el trabajo de manera irreversible”¹¹⁵. Afrontar de un modo decisivo los desafíos que vienen hará depender el contrato social del futuro. Y en el sistema que planteo en este trabajo, si siguen leyendo lo entenderán, nuestros nietos tendrán un salario mínimo nada más nacer. Un pan bajo el brazo.

Los progresistas odian el progreso. Steven Pinker defiende que “la idea de que el mundo es mejor de lo que era”¹¹⁶ y que todavía puede mejorar “pasó de moda” entre intelectuales y eruditos. En la sociedad actual es difícil imaginar ejemplos de cómo será el futuro y ello provoca, lo que los psicólogos Tversky y Kahneman, denominan la “heurística de la disponibilidad”¹¹⁷:

¹¹⁴ Recuperado en <https://www.infotechnology.com/online/Por-que-hay-que-crear-el-Ministerio-del-Futuro-20180910-0009.html>

¹¹⁵ Citado en Vidal, M., La automatización de todo ya ha empezado y es irreversible, recuperado en La automatización de todo ya ha empezado y es irreversible. (marcvidal.net).

¹¹⁶ Pinker, S. *En defensa de la Ilustración*, op. cit.

¹¹⁷ Bazerman, M., *The Relevance of Kahneman and Tversky's Concept of Framing to Organizational Behavior* citado en Bazerman, M.H., Neale, M.A. (1983). *Heuristics in negotiation: Limitations to dispute resolution effectiveness*. In Bazerman, M.H., Lewicki, R.J. (Eds.), *Negotiating in organizations* (pp. 51–67). Beverly Hills: Sage.

evaluamos las posibilidades de algo preguntándonos con que facilidad nos vienen a la mente ejemplos sobre ello.

Resulta curioso comprobar como frente a preguntas tan simples como cuáles son los tres trabajos más peligrosos de nuestro país las respuestas son invariablemente las mismas: transportista, minero y policía. La “heurística de la disponibilidad” es un atajo mental que, ante decisiones complejas, sustituye una respuesta por otra: en vez de responder a la pregunta analizando cada profesión y evaluando su peligrosidad respondemos con los trabajos peligrosos con los que, al pensar en ellos, más ejemplos acuden a nuestra mente. Y la prensa tiene mucho que ver en ello¹¹⁸.

¿Cuáles son los trabajos más peligrosos entonces? Un informe elaborado por la Secretaría de Salud Laboral de CCOO analiza la evolución de los accidentes de trabajo en España desde 2012 del que se comprueba que “el sector servicios es el que acumula un mayor número de accidentes de trabajo en España, independientemente de su gravedad y de si se produce en jornada o in itinere, debido a que supone las tres cuartas parte de la población ocupada”¹¹⁹. Es decir que el trabajo más peligroso es el de camarero. Sin embargo, si observamos la siniestralidad durante la jornada de trabajo nos permite determinar que las profesiones más peligrosas son: minería, obrero de la construcción, operadores de saneamiento, de manufacturas y transportistas. Pero la profesión más azotada es la agricultura.

¿Por qué no incluimos en nuestras respuestas a los agricultores? Por culpa de la heurística de la disponibilidad cuya principal afectación se debe a los medios de comunicación. La prensa

¹¹⁸ Gilovich, T, Griffin, D and Kahneman, D, *Heuristics and Biases: The Psychology of Intuitive Judgment*, Cambridge University Press, 2002.

¹¹⁹ Recuperado de a80ee51cb0e75fce994ded3dde4012c7000001.pdf (ccoo.es)

distorsiona nuestra visión del mundo. Azuzan el imaginario colectivo del progreso con su propia forma de ver el mundo y la cobertura de los accidentes de tráfico mientras los accidentes en el campo no tienen cobertura mediática. Las películas añaden al sesgo la peligrosidad del trabajo de policía cuando en nuestro país su trabajo no es peligroso. Y algo parecido ocurre con los datos y el miedo a la pérdida de nuestra privacidad. Los medios titulan: “la privacidad está muerta” (El País), “El derecho a la intimidad en peligro” (Cantabria TV), “la privacidad perdida” y muchos otros. Pero les aseguro que lo que viene es mejor. Sabremos cómo proteger nuestros datos cuando sepamos cómo se usan. Hasta que Facebook y Cambridge Analítica no fueron descubiertos no sabíamos cómo se utilizaban nuestros datos para condicionar nuestro voto. Hoy lo sabemos. Ganó Trump.

Los datos generan temor y populismos

El artífice del triunfo electoral de Trump, Steve Bannon es uno de los impulsores de la agenda opositora a la Unión Europea y lo que él llama “los intereses de Angela Merkel y Macron”¹²⁰. Cambridge Analytica, cofundada por él, impulsó cientos de *fake news*, sobre todo en Facebook, durante numerosos procesos electorales en todo el mundo. Bannon se ha acercado a líderes como “Salvini en Italia, Le Pen en Francia, y Boris Johnson en Reino Unido”¹²¹. Es precisamente el populismo el peligro del

¹²⁰ Recuperado en La huella de Bannon tras el histórico triunfo de Vox en España (lapoliticaonline.com)

¹²¹ En marzo de 2019 Bannon concedió una entrevista a El País en donde habló de su visión del movimiento nacionalista europeo. En aquel momento identificó al italiano Matteo Salvini y el primer ministro húngaro Viktor Orbán como “los dos políticos más importantes de Europa” y los “líderes ideológicos” del movimiento nacional-populista europeo. Antes de las elecciones de España, el propio Bannon pronosticó que Vox podría “llegar al 15% y eso generaría una onda expansiva en Europa. ¡Un partido que sale de la nada!”. Las campañas políticas de Vox son muy similares a la que hizo Trump en 2016: manejo de redes a través de cuentas falsas y la difusión de noticias falsas para motivar el voto del miedo. Se trata de la misma estrategia que se vio en EU y antes en la campaña del Brexit en Reino Unido. Gracias al conocimiento han aparecido medios para detectar *fake news* y los gobiernos están poniendo coto a estos métodos. Incluso Facebook se ha puesto a favor de la información real. Las campañas políticas de Vox son muy similares a la que hizo Trump en 2016: manejo de redes a través de

progreso y la definición del pesimismo, no los datos y el progreso en sí mismos. Hoy lo que define la percepción del futuro son los titulares y las anécdotas en lugar de los datos los estudios. “Hay una equiparación absurda entre el pesimismo y la sofisticación. Los pesimistas son considerados más serios y moralmente superiores. Tienen prestigio intelectual”, señala Pinker¹²².

Mi positivismo no pretende ocultar la realidad. “Por razones que nunca he entendido, a la gente le gusta escuchar que el mundo se va al infierno”, afirmaba recientemente el historiador Deirdre N. McCloskey al *New York Times*¹²³: “Se que de mí se espera que no sea ingenuo y que defienda que el terrorismo aparecerá con los robots”. Pero no es así. Matt Ridley lo señala en ‘El optimismo racional’: “Si usted dice que el mundo ha ido a mejor corre el riesgo de que le llamen ingenuo e insensible. Si afirma que el mundo va a mejorar, se le considera vergonzosamente loco. Si por el contrario afirma que la catástrofe es inminente, puede esperar un premio McArthur o incluso el Nobel de la Paz”¹²⁴. Aparentemente, “sólo el pesimismo suena profundo. El optimismo suena superficial”, señala la profesora de Harvard, Teresa Amabile¹²⁵.

El futuro está en la cesión de los datos de carácter personal

“El optimismo suena como un argumento de venta, mientras que el pesimismo suena como alguien que trata de ayudarte”,

cuentas falsas y la difusión de noticias falsas para motivar el voto del miedo. Se trata de la misma estrategia que se vio en EU y antes en la campaña del Brexit en Reino Unido. Gracias al conocimiento han aparecido medios para detectar *fake news* y los gobiernos están poniendo coto a estos métodos. Incluso Facebook se ha puesto a favor de la información real. Citado en La Huella de Bannon, op. cit.

¹²² Pinker S, op. cit.

¹²³ Citado en El País recuperado en Por qué el pesimismo nos parece inteligente y el optimismo, simple | Bienestar | BuenaVida | EL PAÍS (elpais.com)

¹²⁴ Ridley, M, op. cit.

¹²⁵ Capitalbolsa, ¿Por qué las opiniones pesimistas parecen más inteligentes que las optimistas?, recuperado en ¿Por qué las opiniones pesimistas parecen más inteligentes que las optimistas? - Bolsamania.com

señaló Housel¹²⁶. Pero debemos entender que la ayuda vendrá de los datos y de la cesión de intimidad. El futuro está en la cesión de la privacidad a cambio de progreso. Ello no nos llevará a la desnudez ni mucho menos a la pérdida de la integridad moral, tampoco, como algunos han dicho que, si cedemos nuestros datos, “vendemos nuestra alma”. La compraventa del uso nuestros datos, el consentimiento informado y la transparencia en su gestión conducirá, simplemente, al avance, a la transformación digital. El pesimismo intentará a poner coto al optimismo y a dar voz a los que reclaman una hiper protección de la intimidad. Y son los intelectuales, los que deben liderar la defensa del progreso, porque tienen la responsabilidad de que nuestro modelo de contrato social funcione. Son los intelectuales, los que deben intelectualizar, valgan la redundancia, la necesidad de controlar nuestros datos y comerciar con ellos. Lo gratis, como dice el profesor Morales, es lo contrario al progreso en una sociedad capitalista.

Y, permítanme, utilizar a un grupo social minoritario pero poderoso: el de la inteligencia de la información. Los analistas tendemos a desnudar al otro de secretos y a sacar a la luz datos que se querían mantener ocultos. No olviden, como he dicho, que todos tenemos una personalidad pública, otra privada y una secreta. Y la secreta se debe mantener ahí donde está. Pero la privada será la que nos permita defender una personalidad pública evolucionada y perfeccionada, en clave de igualdad. Que discutamos, ahora, sobre el futuro sin datos nos llevará al pasado. Sé que mantener lo contrario y haberme mostrado pesimista habría sido más sencillo. Pero no busco elogios sino progreso.

¹²⁶ Citado en Capitalbolsa, ¿Por qué las opiniones pesimistas parecen más inteligentes que las optimistas?, op. cit.

Decía Thomas Hobbes en 1651 que “en la competencia por el elogio hay una inclinación a reverenciar la antigüedad” (*Leviatan*)¹²⁷. Pero también sostiene que entre las pasiones que con mayor frecuencia causan los delitos son la vanagloria personal. Si los unimos ambos conceptos estamos ante una Tercera Guerra Mundial. “*So that in the nature of man, we find three principal causes of quarrel. First, competition; secondly, diffidence; thirdly, glory*”¹²⁸. Strauss lo señala:” el origen del apetito del hombre no es la percepción sino la vanidad”¹²⁹. El día que nuestros políticos alcen la mirada ese día progresaremos, a pesar de que haya voces que adviertan que hemos vuelto al Oeste americano. Es el momento de vender nuestros datos y progresar. Pero venderlos bajo un contrato social de mera licencia de uso que nos proteja y establezca los límites.

Internet la nueva tierra de los comunes

Imaginemos que un grupo de campesinos se une para facilitar un terreno donde sus animales pasten. Un día uno de ellos, necesitado de dinero, adquiere un animal extra y lo lleva a pastar con el resto. Sabe que no es bueno para el terreno, pero sus intereses personales son acuciantes. Como la cosa funciona otro día aparece otro campesino con un nuevo animal. Sus compañeros hacen lo propio hasta que el terreno deja de tener hierba. Esto se conoce como la parábola de los campesinos cuya formulación pertenece al escritor británico William Forster Lloyd que, posteriormente, fue adoptada por el biólogo neomalthusiano Garret Hardin en «The Tragedy of the Commons»¹³⁰:

¹²⁷ Hobbes, T, *Leviatan*, edición Deusto, 2002.

¹²⁸ Citado en Hobbes' *Leviathan*” in William Ebenstein, *Great Political Thinkers: Plato to the Present* (New York: Holt, Rinehart, and Winston, 1969), pp. 372–74

¹²⁹ Citado en Korstanje, M., *El temor en Thomas Hobbes como organizador político: Notas preliminares sobre la paradoja profesional*, en *Revista Internacional de Filosofía*, vol. XV (2010), pp. 167-186

¹³⁰ Hardin, G, *The tragedy of the Commons*, *Science*, 1968, Vol. 162, Issue 3859, pp. 1243-1248

“Aquí yace la tragedia. Cada hombre está atrapado en un sistema que le empuja a aumentar su rebaño sin límite... en un mundo limitado”. El beneficio personal en detrimento del colectivo ha acabado con los recursos naturales. Los intereses egoístas a corto plazo son incompatibles con los intereses colectivos a largo plazo del bien común. El ensayo de Hardin, publicado el 13 de diciembre de 1968 en la revista *Science*, tuvo un enorme impacto entre los economistas que durante años sostuvieron que los recursos naturales de uso colectivo inevitablemente derivan en una sobreexplotación hasta su agotamiento. Algunos ejemplos de la tragedia de los comunes en la actualidad los azuza la niña activista Greta Thunberg allí donde habla: la sobreexplotación de los recursos marítimos, la resistencia a los antibióticos o la creación de autopistas para evitar la congestión urbana. En definitiva, el calentamiento global y el cambio climático: “Nuestra biósfera se está sacrificando para que las personas ricas en países como el mío puedan vivir de lujo. Son los sufrimientos de muchos los que pagan por el lujo de unos pocos”¹³¹.

En este escenario, Internet es la nueva «tierra» en la que los recursos comunes se pueden agotar. Muchas de los nuevos tecnólogos utilizan el ejemplo de la parábola de Hardin para exigir una Internet libre de intervenciones. La Declaración de Libertad en Internet es una declaración en línea del año 2012 en defensa de las libertades entre cuyos firmantes están Amnistía Internacional, *Electronic Frontier Foundation*, Reporteros Sin Fronteras, y la Fundación Mozilla. La declaración apoya el establecimiento de cinco principios básicos:

- Internet sin censura.
- Acceso universal a redes rápidas y asequibles.

¹³¹ Greta Thunberg ante la Cumbre del Clima de las Naciones Unidas, 2018

- Libertad para conectarse, comunicarse, crear e innovar en Internet.
- Protección para nuevas tecnologías nuevas e innovadoras sin el abuso de los usuarios.
- Derechos a la privacidad y la capacidad para el usuario de Internet de controlar que información suya está siendo utilizada.

La nueva red de redes es un bien común que debe ser estudiado y protegido de la voracidad de unos pocos se vendría a decir siguiendo la teoría de la ‘Tragedia de los Comunes’. Daniel McFadden, Premio Nobel de Economía del año 2000, cree que el manejo de estos “commons” se creará una dura batalla para decidir la forma en que se tendrá acceso a la información común, posiblemente, entre las opciones de servicios basados en el proveedor de servicios de Internet (ISP), por los que los usuarios deberán pagar una tarifa mensual, y la de un monopolio (Microsoft) que cobraría a través de la licencia pagada por el sistema operativo¹³². Algunos no están de acuerdo.

La politóloga y premio Nóbel Elinor Ostrom investigó durante más de dos décadas los problemas de la gestión colectiva y cuestiona teórica y empíricamente este pensamiento económico: “Ni el Estado ni el mercado han logrado un éxito uniforme en que los individuos mantengan un uso productivo, de largo plazo, de los sistemas de recursos naturales. Por otra parte, distintas comunidades de individuos han confiado en instituciones que no se parecen ni al Estado ni al mercado para regular algunos sistemas de recursos con grados razonables de éxito durante largos periodos”¹³³. Esta fue, precisamente, la aportación destacaba por el Comité del Nobel al explicar la concesión del galardón, compartido con el economista Oliver E. Williamson: “Elinor Ostrom ha puesto en cuestión la afirmación conven-

¹³² McFadden, D, The Tragedy of Commons, Forbes, 200 recuperado en Forbes.com - Magazine Article

¹³³ Ostrom, E, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press, 2015.

cional de que la gestión de la propiedad común suele ser ineficiente, razón por la cual debería ser gestionada por una autoridad centralizada o ser privatizada. A partir de numerosos estudios de casos de manejo por parte de sus usuarios de bancos de pesca, pastizales, bosques, lagos, y aguas subterráneas, Ostrom concluye que los resultados son, en la mayoría de los casos, mejores que en las predicciones de las teorías estándar. Sus investigaciones revelan que los usuarios de estos recursos desarrollan con frecuencia sofisticados mecanismos de toma de decisiones, así como de resolución de conflictos de intereses, con resultados positivos”¹³⁴.

Por tanto, se puede concluir que es posible manejar bienes comunes de manera eficiente sin llegar a la tragedia, a pesar de que en derecho deberíamos hablar de “terribilidad” frente a un derecho, el de la propiedad, que parafraseando a Jeremy Bentham cuando señala en su *Principles of the Civil Code* al deseo de ser propietario. Terrible porque ese deseo enfrentaría a quienes no son propietarios con los que sí lo son; y es el Derecho quien debe aquilatar los deseos con los derechos¹³⁵. Pero vayamos un paso más allá. ¿Podemos negociar la tragedia? La respuesta es sí. En derecho todo es negociable salvo la vida¹³⁶. En este sentido, Ronald Coase, uno de los padres fundadores del análisis económico del derecho, en su “Teorema de Coase”¹³⁷ establece que, en algunos casos, aunque una negociación sea beneficiosa para un grupo de personas no se llega a un acuerdo.

¹³⁴ Ramis, A., El concepto de bienes comunes en la obra de Elinor Ostrom, *Ecología política*, N° 45, 2013, págs. 116-121

¹³⁵ En *The Works of Jeremy Bentham*, Bowring (ed.), Thoemmes Press, Bristol, 1995 citado por Villarde I, en *La Intimidad, ese terrible derecho en la era de la confusa publicidad virtual*, Chapecó, v. 14, n. 3, p. 57-72, Edição Especial, 2013.

¹³⁶ La discusión sobre el balanceo de derechos y la imposibilidad de renunciar al derecho de la vida es una discusión más profunda, más tras la aceptación de la eutanasia en determinadas legislaciones nacionales.

¹³⁷ Ronald Coase. El problema del Costo Social, *The Journal of Law and Economics* (octubre 1960), pp. 1-44.

Estos impedimentos a los que llama “los costos de una transacción”. Una negociación triunfa si los costos legales son nulos. A la inversa, fracasa.

Los tecnólogos han adoptado la tragedia de los comunes y la han llevado a su discurso sobre el habeas data. “La privacidad del consumidor también es un recurso escaso que sufre la tragedia de los bienes comunes. Impulsadas por los ingresos publicitarios, las corporaciones se volvieron cada vez más eficientes en la recopilación y el uso de datos del consumidor para dar forma al comportamiento del consumidor. En 2016, vimos estos datos utilizados para manipular a las personas con el objetivo de influir en las decisiones políticas. Cambridge Analytica aprovechó los datos de Facebook de millones de ciudadanos para afectar el resultado del voto Brexit y las elecciones presidenciales de Estados Unidos. Esta falta de privacidad de datos ahora ha comenzado a impactarnos a todos”¹³⁸.

En España el discurso se ha mantenido por autores como Rodríguez¹³⁹ siguiendo a Nikolaos Laoutaris que en su seguido artículo *Cows, Privacy, and Tragedy of the Commons on the Web*, establece una analogía clara con la parábola neomaltusiana. El punto principal aquí es que si los modelos de negocio (agricultores) y las tecnologías (vacas) mencionados anteriormente consumen la confianza del usuario (pasto) más rápido que su tasa de reposición (servicios gratuitos que nos hacen felices), en algún momento la confianza se dañará más allá reparación y usuarios... “simplemente abandonarán la web”¹⁴⁰. Lo que es aún peor, tal pérdida de confianza puede ser causada por las acciones de una minoría de empresas (incluso pequeñas) que

¹³⁸ <https://steemit.com/blockchain/@bornswift/data-privacy-and-the-tragedy-of-the-commons>

¹³⁹ Rodríguez, P, *Inteligencia Artificial: cómo cambiará el mundo (y tu vida)*, Deusto, 2018.

¹⁴⁰ Loutaris, N., *Cows, Privacy, and Tragedy of the Commons on the Web*, recuperado en *Cows, Privacy, and Tragedy of the Commons on the Web – Nikolaos Laoutaris*

al involucrarse en prácticas de recolección de datos cuestionables y ofensivas puede dañar a toda la industria, incluida la mayoría de las empresas que son sensibles a los usuarios 'requisitos de privacidad.

Los impuestos y las regulaciones ha sido la solución recurrente para la tragedia del problema de los bienes comunes y de ellos debemos huir, ya que eso sí nos adentraría en la tragedia de los comunes. Porque, como ya he dicho y ampliaré más adelante, la única solución parte del consentimiento, de la transparencia y de la seguridad. El Reglamento Europeo de Protección de Datos Personales, que también se analizará más adelante, es un claro ejemplo hacia dónde estamos caminando y donde no debemos caminar. Pero déjenme que adelante unas pequeñas conclusiones: los humanos tendremos, como he dicho, una personalidad digital y con ella haremos lo que queramos. Las empresas dejarán de facilitar gratuitamente información a cambio de esos datos que cedemos, sin más. Los hombres valoraremos los datos, los venderemos y a cambio obtendremos servicios. Tendremos una especie de contabilidad humana desde nuestro nacimiento como personas digitales, un debe y un haber donde ingresaremos dinero digital y pagaremos con él. Y todo ello deberá ser transparente con las empresas, dejando al Estado y a una entidad supranacional, como en el contrato social, la protección de dichas transacciones mientras alejamos a las cinco grandes corporaciones que seguirán viviendo pero pagando por el pasto (los datos) que usen.

Facebook continuará (si lo hace) con sus empresas, pero nos pagará por estar en sus redes. Nosotros a cambio, pagaremos con nuestros datos o con recursos económicos por utilizar sus recursos. Y el Estado, que también se beneficiará de todo ello, deberá proteger nuestra hucha digital, nuestra caja de seguridad de datos personales que está en peligro.

Los nuevos peligros y la justicia privada

Las amenazas acechan en cualquier lugar digital. Estudios sobre la vulnerabilidad demuestran que todo es accesible. Es posible robar un Audi TT en diez segundos, un Land Rover en treinta, señala un estudio de la seguridad de los nuevos vehículos con cerraduras digitales. Entrar en casas con cerradura digital, vulnerar alarmas, saltarse accesos digitales como antaño se descerraban cerraduras o se rompían cráneos con piedras. Hasta aquí nada nuevo en la Humanidad. Los mismos rateros, los mismos peligros.

Sin embargo, hay otros delitos y estos permanecen ocultos. Ladrones en Chicago robaron cien coches de una compañía de *car sharing*, ciberdelincuentes accedieron a controlar online un marcapasos, chips infectados, espionaje entre empresas para saber dónde están situados los coches y poner los suyos a disposición del usuario, secuestro de datos a abogados, filtraciones de secretos, hackeo sin más, copias digitales perfectas son alguno de los problemas con los que nos encontraremos en el futuro. La diferencia es que muchas de estas brechas de seguridad no las conoce ni la policía, ni la justicia y mucho menos la prensa. Las empresas las mantienen ocultos de las miradas de la sociedad. Los gobiernos ocultan ciberataques globales salvo que intereses para su política común, como por ejemplo, las amenazas al Gobierno Chino¹⁴¹.

Parece que lo que los demás no ven no existe. Pero sí, los riesgos están ahí y no desaparecen por mucho que los mantengamos lejos de la mirada del escrutinio público. La pregunta es ¿cómo lo han conseguido? Privatizando la justicia: detectives privados, abogados y tribunales de arbitraje mantienen a los medios de

¹⁴¹ EE.UU. y la UE acusan a China de estar detrás del ciberataque a Microsoft (yahoo.com)

comunicación ciegos de información. Algo que, a priori, no es bueno ni malo. Pero que debe ser objeto de estudio. Si en la Ilustración las penas dejaron de ser expiatorias y el Estado tenía en exclusiva el *ius punendi*, debemos comprobar hasta qué punto el sistema sigue siendo viable.

¿Se debe privatizar la seguridad? ¿Y la justicia? Ese sería el verdadero cambio del contrato social: volver a pagar por algo por lo que ya se pagó al acceder al contrato social cediendo parte de nuestra libertad. Para evitar la represión, la injusticia de las penas morales, de las cárceles eternas nuestros ancestros dejaron de ser libres. Hoy, algunos mantienen que la justicia debe ser privada. Otros que es un oximoron. Anthony Kline, juez de apelación de California, mantiene que las empresas y los árbitros tienen una razón económica para decidir en favor de los jugadores que más veces son demandantes o demandados. El arbitraje es un método alternativo de resolución de conflictos donde las partes pueden decidir no someter su controversia a la jurisdicción de un país, sino a la tutela de un tribunal de arbitraje privado. Recientemente, se ha cuestionado el sistema al mantener que únicamente benefician a multinacionales en defecto de los ciudadanos. Un reportaje en tres entregas en *The New York Times*¹⁴² pone de manifiesto que millones de ciudadanos norteamericanos han renunciado a su derecho constitucional para acudir siquiera un día a los tribunales aun sin saberlo, debido a que firman contratos con cláusulas individuales de arbitraje en los contratos de empleo. Cláusulas en las de tarjetas de crédito, en el uso de los coches de *car sharing*, en los sistemas de seguridad y en tantos contratos privados que parece ilógico que el Estado no proteja al consumidor. El problema no radica en el sistema sino en la transparencia del sistema.

¹⁴² In Arbitration, a 'Privatization of the Justice System' - *The New York Times* (nytimes.com)

El arbitraje se ingenió por una coalición de empresas de tarjetas de crédito que deseaban aislarse del escrutinio público de los tribunales y de su alto coste procesal. Estudios internacionales demuestran que los motivos por los que algunos delitos llegan a arbitraje son¹⁴³:

- Las empresas privadas pueden tener mayor experiencia y recursos que las fuerzas públicas para investigar y resolver ciertas clases de delitos, por ejemplo, los fraudes informáticos o los levantamientos de velo societario transnacional.
- La empresa involucrada suele no desear la publicidad negativa derivada de la difusión de estos hechos.
- La resolución privada de ciertos delitos es mucho más rápida.
- Para la empresa involucrada, puede ser más caro acudir al sistema público de justicia que resolver el tema por sus propios medios. La empresa puede tomar la decisión de simplemente pagar una prima de seguro un poco mayor, o pasar los costes de estos delitos a sus clientes como precios más altos. Ocurre en los costes de pérdida desconocida en los supermercados o en las primas de seguro.

¿Tiene sentido el contrato social con una justicia privada? La respuesta es no. ¿Tiene sentido la justicia privada en el mundo de la empresa 4.0? Sí, las empresas no firman el contrato social, solo las personas. Aunque la libre empresa, la competencia leal, los derechos al trabajo y al trabajo digno formen parte del contrato social, éste no contempla a las personas jurídicas como tal. Por tanto, la privatización de la justicia que afecte a las sociedades no es ningún contrasentido. Un “país no puede funcionar sin gobierno, pero el gobierno no puede solucionar todos los

¹⁴³ La información siguiente aparece referenciada en Frigo, E., El Poder judicial privado, obtenido en Artículo: El Poder Judicial privado : La privatización de la justicia (gestiondelriesgo.com)

problemas”¹⁴⁴. Ni el sector privado ni el público son la respuesta. No se trata de uno o de otro, se trata de las dos cosas. Se trata de usar al sistema privado y de estar protegido por el público. Porque para algunos los monopolios tecnológicos están secuestrando nuestra vida.

Por ello los ciudadanos debemos empezar a batallar con las empresas tecnológicas para que nos devuelvan nuestros datos y empezar a negociar con ellos (los datos) protegidos por una entidad Supranacional y nuestros Estados. Así, vendiendo (o cediendo el uso) y comprando datos de forma segura podremos no perder el tren del futuro y convertirnos en homeless digitales, que deberán ser protegidos por el Estado mediante el contrato social analógico.



¹⁴⁴ Rosling, H, *Factfulness: Diez razones por las que estamos equivocados sobre el mundo. Y por qué las cosas están mejor de lo que piensas*, Planeta, 2018.

❖ CAPÍTULO 6. LOS DERECHOS EN LA QUINTA REVOLUCIÓN INDUSTRIAL Y LOS TECNOAGOREROS

Alemania está estudiando el futuro código de circulación para adaptar las normas al coche autónomo. El debate se centra en determinar quién es el titular responsable de los problemas derivados de su uso. El debate pretende determinar si quien fabrica, distribuye o comercializa el vehículo es responsable per se, o, únicamente por su uso. Parece un debate nuevo, pero no lo es.

La responsabilidad objetiva o teoría del riesgo creado es una fuente de obligaciones reconocida¹⁴⁵. Los defensores de esta teoría señalan que el que “hace uso de cosas peligrosas, debe reparar los daños que cause, aun cuando haya procedido lícitamente”¹⁴⁶. El debate, como he señalado, no es nuevo y está superado. El principio de culpabilidad (“*nullum crimen sine culpa*”) es un pilar fundamental de todo Estado de Derecho, que sin duda representa un límite a la potestad punitiva del Estado que nos trajo la Ilustración. La exclusión de la responsabilidad objetiva en el concepto de delito no se apreciaba en el artículo 1 del antiguo Código Penal de 1973, no obstante, tras la reforma de 1983, la cláusula definitoria del delito se destinó a excluir la responsabilidad objetiva, mediante la exigencia del dolo o la culpa, y desde entonces, tanto la doctrina penal española como la jurisprudencia, han proclamado de forma reiterada tal exclusión de la responsabilidad objetiva. Los criterios que sancionan la peligrosidad sin delito por el simple “estado peligroso”

¹⁴⁵ Sobre la definición jurídica de este concepto véase Responsabilidad objetiva o riesgo creado (definicionlegal.blogspot.com)

¹⁴⁶ Responsabilidad Objetiva o Riesgo creado recuperado en 8.pdf (unam.mx)

de Garófalo (1880) apunta a “la perversidad constante y activa del delincuente” o del autor (“la muy relevante probabilidad de la persona de convertirse en autor de un delito”) han sido descartados porque representan un castigo sin acto, sin delito, por un simple modo de ser, algo arbitrario y propio de los regímenes autoritarios.

Por eso surge la responsabilidad extracontractual. “De los riesgos generados por la actividad humana, el específico de la conducción aparece como uno de los más cercanos, de los más habituales, con el que todos coexistimos, ya sea generándolo o sufriendo sus consecuencias en forma de daños. Por su frecuencia, se trata de un riesgo que tiene un enorme impacto en la realidad social y económica de un país.” En tales términos se pronuncia el Preámbulo de la Ley 35/2015, de 22 de septiembre, de reforma del sistema para la valoración de los daños causados a las personas en accidentes de circulación. Durante la tramitación del Proyecto que daría lugar a la Ley 35/2015 se planteó la cuestión de la naturaleza jurídica de la responsabilidad contemplada en el art. 1.1, debatiéndose si el texto respondía o no a un sistema de responsabilidad objetiva por el hecho circulatorio o si se trataba solo de una inversión de la carga de la prueba de la culpa.

Existe, por tanto, una responsabilidad cuasi objetiva en materia civil que se concreta en la presunción de culpa del conductor de un vehículo a motor salvo que se pruebe que los daños fueron debidos únicamente a la conducta o la negligencia del perjudicado. Existe, por tanto, una inversión de la carga de la prueba en situaciones de creación de riesgo. ¿Por qué? Porque existe el error humano.

Pero si el fabricante no será responsable penal de los vehículos sin fallos y no existe el error humano ¿quién será el responsable

civil? El responsable del uso de los vehículos autónomos acabará siendo el titular de los derechos públicos de las *smartcities*. Existirá una penalización a la ineficiencia. La posibilidad de que la IA pueda poner en riesgo la humanidad es un *prius* ampliamente aceptado. Los tecnoagoreros están aquí. Elon Musk, fundador de Paypal y consejero delegado de Tesla Motors y la compañía aeroespacial SpaceX, es considerado como uno de los principales protagonistas de la innovación y el mayor defensor de la existencia de riesgos existenciales ciertos para la humanidad. “Hasta que la gente no vea a los robots matar a personas por la calle no se entenderán los peligros de la inteligencia artificial”. “Es un riesgo para la existencia de nuestra civilización”¹⁴⁷, ha manifestado públicamente con un eco que parece haberse convertido en una realidad cierta.

La vida en la Tierra acabará en cuanto la Inteligencia Artificial sea parte de nuestra vida es el mensaje de los tecnoagoreros como Musk o Hawking que en 2017 advirtió en Lisboa: “Las computadoras pueden, en teoría, emular la inteligencia humana e incluso excederla”, advirtió el cosmólogo británico. “La creación exitosa de una IA efectiva podría ser el evento más grande en la historia de nuestra civilización. O el peor. Simplemente no lo sabemos. Por lo tanto, no podemos saber si seremos infinitamente asistidos por la IA, o si seremos ignorados y marginados, o posiblemente destruidos por ella”¹⁴⁸.

En 2018, más de cien líderes en el área de robótica e IA, entre ellos Elon Musk; Mark Zuckerberg, fundador de Facebook; o Mustafa Suleyman, cofundador de DeepMind de Google, firmaron una Carta Abierta a la Convención de las Naciones Unidas sobre Ciertas Armas Convencionales, en la que advierte de

¹⁴⁷ Elon Musk: “Hasta que la gente no vea a los robots matar a personas por la calle no se entenderán los peligros de la IA” | Tecnología | ComputerWorld

¹⁴⁸ Stephen Hawking advierte sobre el desarrollo de la inteligencia artificial - SDI (nationbuilder.com)

la necesidad de establecer un grupo de expertos sobre sistemas letales de armas autónomas, ya que las tecnologías de inteligencia artificial y robótica pueden ser reutilizadas para desarrollar armas autónomas que pueden poner en peligro a la humanidad: “Estas pueden ser armas de terror, armas que los déspotas y terroristas usen contra poblaciones inocentes, y armas hackeadas para comportarse de manera no deseada [...]. Una vez que se abra esta caja de Pandora, será difícil cerrarla”¹⁴⁹.

La lucha por seguir vivos es un impulso biológico en todos nosotros. Sé que el deseo de prolongar la vida es una de las metas que se pronostican más certeras en los siguientes veinticinco años. Ray Kurzweil pronostica en “La Singularidad está cerca”¹⁵⁰ que en 2045 seremos algo así como inmortales gracias a los avances en genética, nanotecnología y la IA. Y ahora que parece que lo conseguimos llega otra amenaza: los robots malvados.

Pinker¹⁵¹ señala entre los riesgos existenciales que “supuestamente amenazan el futuro de la humanidad figura una versión del siglo XIX del efecto 2000”. El pesimismo cala en nuestro cerebro tal y como las sectas captan adeptos. Nuestro cerebro trabaja simplificando la realidad. Las explicaciones sencillas, cortas y resolutivas tienen un gran poder de enganche. Por eso, como ya he dicho, los populismos y nacionalismos crecen en todo el Planeta salvo en la masa poblacional ilustrada. En España los partidos independentistas y aquellos de corte neofascista o marxista han calado hondo por la simpleza del mensaje. La principal causa del auge es de raíz económica. Tras una larga, brusca y profunda recesión económica entre 1995 y 2013, estos movimientos surgieron como nuestra salvación. El meca-

¹⁴⁹ Recuperado en ¿Es la inteligencia artificial el nuevo peligro para la humanidad? (lasexta.com)

¹⁵⁰ Kurzweil, R, La singularidad está cerca, Lola Books, 2021.

¹⁵¹ Pinker, op. cit.

nismo de captación de adeptos es sencillo: se inocula el veneno mediante la semiótica. En el caso de Podemos se abre un puente social entre el pueblo y la “casta”. En el nacionalismo catalán “España nos roba”. Vox con el sempiterno y siempre útil “los de fuera nos quitan el trabajo”. Hannah Arendt, Victor Klemperer, George Orwell y otros pensadores del siglo XX, como George Steiner, quisieron demostrar que el totalitarismo “es una cultura política íntimamente ligada a la corrupción del lenguaje, y a su vez la corrupción del lenguaje establece los cimientos del totalitarismo”¹⁵².

En ‘La lengua del Tercer Reich’, Victor Klemperer señala: “las palabras pueden actuar como dosis ínfimas de arsénico: uno las traga sin darse cuenta, parecen no surtir efecto alguno, y al cabo de un tiempo se produce un efecto tóxico”. Este filólogo creía que la retórica fue lo que permitió la masacre judía. El discurso populista es simple y no se dirige al intelecto sino a las emociones. Según Klemperer “cruza la frontera hacia la demagogia o hacia la seducción de un pueblo cuando pasa de no suponer una carga para el intelecto a excluirlo y narcotizarlo de manera deliberada”¹⁵³.

Inoculado el veneno solo queda el antídoto: el populismo. Pues bien, algo así ocurre en la actualidad con el discurso tecnoagorero. Han inoculado su veneno y ahora esperan dar soluciones. Pronto existirá algún partido político que lleve en su programa electoral la lucha contra los robots y la IA que aniquilará nuestro mundo, cuando la mayoría de los expertos en IA piensan lo contrario. Investigadores de la Universidad de Oxford decidieron tratar de separar la señal del ruido para averiguar la reali-

¹⁵² Casabon, C., El Lenguaje del Populismo. Letras Libres recuperado en La lengua del populismo | Letras Libres

¹⁵³ Recuperado en El lenguaje del proceso (lavanguardia.com)

dad. Se encuestaron a quinientos cincuenta destacados expertos en inteligencia artificial y descubrieron que mientras que poco más de la mitad se mostraron optimistas, prediciendo que la IA en última instancia, era “bueno” o “muy buena” solo uno de cada tres pensó que sería “malo” y uno de cada cinco creen que sería “muy malo (una amenaza existencial).

También es cierto que no podemos mirar al futuro con la visión antropocéntrica del pasado. El filósofo alemán Hans Jonas recurre a la “heurística del temor”¹⁵⁴. Jonas considera que la posibilidad de que provoquemos algún desastre ecológico es muy alta, y que las consecuencias de un desastre de este tipo podría afectar dramáticamente a nuestra existencia como seres humanos, corriendo riesgo incluso de desaparecer. Y parece que la historia actual le da la razón: el coronavirus, Chernobil, la crisis de las vacas locas.

Un estudio del Servicio de Estudios del Parlamento Europeo¹⁵⁵ analiza en profundidad estos riesgos y, de forma previa, aboga por destruir tres mitos antes de abordar el problema:

- Algunos analistas creen que existe un cierto peligro en que una IA «se suelte» y «se haga superinteligente» (Häggström)¹⁵⁶. La primera ley de la IA nos dice que la inteligencia artificial es un objetivo tremendamente difícil, que requiere las condiciones exactamente adecuadas y un esfuerzo considerable. No habrá inteligencias artificiales fugitivas ni tampoco inteligencias artificiales con un desarrollo propio que escapen a nuestro control. No habrá singularidades. La IA solo alcanzará el

¹⁵⁴ Citado en Restrepo, JC, *La teoría de la responsabilidad como imperativo ético. Hans Jonas y el principio axiológico para la tecnociencia*, Fac. Filos. Let. Univ. Pontif. Bolívar. vol.19 no.42 Bogotá Jan./July 2011

¹⁵⁵ Boucher, P, ¿Debemos temer a la Inteligencia Artificial?, Servicio de Estudios del Parlamento Europeo, 2018.

¹⁵⁶ Häggström, O, y otros en ¿Debemos temer a la inteligencia artificial?: análisis en profundidad, recuperado en ¿Debemos temer a la inteligencia artificial?: análisis en profundidad (uji.es).

- grado de inteligencia que nosotros le animemos (u obliguemos) a alcanzar, bajo fuerte presión.
- Segundo mito: con recursos suficientes (neuronas/ordenadores/memoria), una IA será más inteligente que los humanos. La segunda ley de la IA nos dice que los recursos no son suficientes. Seguimos teniendo que diseñar nuevos algoritmos y estructuras dentro de las IA y como apoyo para cada nueva dificultad a la que se enfrenten.
 - Tercer mito: puesto que la velocidad de los ordenadores se duplica cada dieciocho meses, las IA explotarán este poder de computación y se volverán exponencialmente más inteligentes. La tercera ley de la IA nos dice que, a medida que aumenta la inteligencia, el tiempo necesario para el ensayo puede incrementarse exponencialmente. En última instancia, el ensayo puede imponer límites prácticos a una inteligencia artificial viable y fiable. De la misma forma que cada vez es más difícil ir más rápido a medida que nos acercamos a la velocidad de la luz, cada vez es más difícil aumentar la inteligencia mientras construimos cerebros más inteligentes.

Aterrador y peligroso son dos cosas distintas. “Algo aterrador plantea un riesgo percibido. Algo peligroso plantea un riesgo real”, señala Rosling¹⁵⁷. Centrar nuestra atención en lo aterrador en lugar de lo peligroso provoca que el mundo no avance y que si lo hace lo haga con miedo. Y ahí es donde entra de lleno el discurso sobre la pérdida de privacidad.

La hiperprivacidad un problema del siglo XXI

Tim Cook, CEO de Apple, manifestó en la Universidad de Stanford que “si aceptamos como normal e inevitable que todo en nuestras vidas puede ser agregado, vendido o incluso filtrado

¹⁵⁷ Rosling, H, Factfulness, op. cit.

por una brecha de seguridad entonces perdemos mucho más que datos. Perdemos la libertad de ser humanos”. “En un mundo sin intimidación digital incluso si no has hecho nada más que pensar diferente empiezas a censurarte. No del todo al principio. Sólo un poco, poco a poco. Arriesgar menos, esperar menos, imaginar menos, atreverse menos, crear menos, intentar menos, hablar menos, pensar menos. El efecto aterrador de la vigilancia digital es profundo y lo afecta todo¹⁵⁸”.

Para Cook la privacidad es uno de los asuntos más importantes del siglo. En una conferencia recogida por la prensa española señala que “hay más datos en tu móvil que en tu casa”. Durante su conversación con Bill McDermott, su homólogo en la europea SAP, señaló la ciberseguridad como un elemento esencial del nuevo siglo: “si los atacantes acceden a un dispositivo móvil de empresa, tienen a su disposición muchísima información sensible o confidencial de la organización. Es algo muy importante”.

¿Cuál es la solución para este reto? En palabras de Tim Cook, todo pasa por una aproximación holística al problema. “La solución es integrar las mejores capacidades de seguridad en el hardware y software que vendemos, de manera que trabajen conjuntamente para ofrecer la máxima protección de datos”. Cook centra la protección del ciudadano en la empresa, otros lo hacen en el Estado y algunos no quieren ni dejar pensar en estas cuestiones al ciudadano, algo que no es nuevo.

A finales del siglo XVIII las máquinas de vapor sustituyeron a los empleados de las fábricas. La electricidad permitió un aumento de la productividad industrial y la sustitución de la mano de obra por maquinaria. Aquello se llamó crisis indus-

¹⁵⁸ Recuperado en Apple's Tim Cook calls on Stanford graduates to take responsibility

trial y acabó con la recolocación de la mano de obra. Negar hoy lo que viene es negar el futuro y no conocer el pasado. Existen, principalmente, tres modelos de contrato social con respecto al *privacy right*: el chino, el sajón y el europeo continental. Veamos cuál debemos adoptar. Los datos, a pesar de lo que Tim Cook, señala no son los nuevos herejes y brujas, son un elemento más de la evolución que deberemos acotar. Pero el futuro sin datos no existe. Los datos son el elemento fundamental de la quinta revolución industrial.

La concepción excesivamente dramática del mundo “es lo que hace que las personas elijan las respuestas más dramáticas y negativas”¹⁵⁹ a las preguntas que nos debemos hacer frente a lo que está por llegar. Solo si nos desembarazamos de lo percibido y analizamos la realidad podremos obtener una respuesta correcta. Vamos a ello.

Seguridad y el sesgo algorítmico

No es tan importante la discusión sobre si podemos (o no) ceder nuestra privacidad como quién protege los datos.

Junto a la propiedad, la libertad es el fundamento de la construcción de nuestra civilización. La libertad como límite al poder. La libertad como exigencia al Estado. Pero los hombres no quieren ser libres, quieren vivir seguros.

Estados Unidos usó el miedo y el peligro tras el 11 M para imponer sus reglas de juego. Lo hemos visto, también, con la crisis económica. La economía se hundió y el ciudadano recurre al Estado. Exige y pide tranquilidad, seguridad y vivienda. ¿A cambio de qué? Si le devolvemos el poder que le quitamos al

¹⁵⁹ Rosling, H, op. cit.

Estado durante la Ilustración surgirán los totalitarismos, como en China. Durante el covid la sociedad demanda del Estado que cubriesen las carencias económicas que surgían del cierre de los establecimientos y de la paralización de la economía. Es la eterna discusión del liberalismo y el socialismo.

Tal y como hemos señalado el contrato social requiere de Estado, pero uno que proteja la libertad y, a la vez, asegure la igualdad interfiriendo lo menos posible en nuestra vida. La obligación del Estado es darnos seguridad sin quitarnos libertad, esto es, sin generarnos miedo. Además, tal y como hemos indicado la cesión de partes de nuestra privacidad no viene dado, tanto, por lo que puedan saber de nosotros sino con que aseguren que no van a utilizar esos datos contra nosotros.

En el año 2015, Jacky Alcine, ciudadana afroamericana, miró su fotografía en la aplicación de Google Photos y no podía creer que el software de reconocimiento facial la había etiquetado con la palabra “gorila”¹⁶⁰. “Esto sucedió porque el algoritmo no había sido entrenado con suficientes imágenes de personas de piel oscura”¹⁶¹. Ese mismo año si se buscaba “la casa del negro” o “rey negro” (en inglés) en Google Maps en los alrededores de Washington DC la aplicación nos dirigía a la Casa Blanca, ocupada por Barack Obama, y por su familia. “Al año siguiente, Microsoft lanzó a “Tay”, un chatbot cuyo fin era imitar el comportamiento de una adolescente curiosa y buscaba entablar en las redes sociales una conversación informal y divertida con una audiencia de entre 18 y 24 años, según explicó la compañía en su página web. En poco tiempo Tay mostraba empatía hacia

¹⁶⁰Recuperado en <https://www.enfoquederecho.com/2019/11/07/el-sesgo-algoritmico-y-la-proteccion-de-datos-personales/>

¹⁶¹ Morales, A, El impacto de la inteligencia artificial en la protección de los datos personales, recuperado en el impacto de la inteligencia artificial en la protección de datos personales (worldcomplianceassociation.com)

Hitler y defendió el Holocausto, los campos de concentración o la supremacía blanca, y se mostró contraria al feminismo”¹⁶².

Como se ha dicho las aplicaciones de inteligencia artificial (IA) basan su aprendizaje profundo en algoritmos especializados en encontrar patrones en los datos. “Lo primero que hacen los informáticos cuando crean un modelo de aprendizaje profundo es decidir cuál es su objetivo. Una compañía de tarjetas de crédito, por ejemplo, podría querer predecir la solvencia de sus clientes, pero “solvencia” es un concepto bastante difuso”.¹⁶³ Pero en muchos casos aparecen los sesgos algorítmicos. “Los datos producen sesgos principalmente por dos vías: o los datos recopilados no son representativos de la realidad o reflejan prejuicios ya existentes. El primer caso podría ocurrir, por ejemplo, si un algoritmo de aprendizaje profundo recibe más fotos de las caras de piel clara que las de piel oscura. El sistema de reconocimiento facial, como consecuencia de eso, sería inevitablemente peor en el reconocimiento de las caras de piel más oscura. El segundo caso es precisamente lo que sucedió cuando Amazon descubrió que su herramienta de reclutamiento interno estaba descartando las candidatas mujeres. Dado que el algoritmo se entrenó a partir de decisiones históricas de contratación que favorecían a los hombres sobre las mujeres, el software aprendió a hacer lo mismo”, señala la revista *Mit Technology*.

La mejor manera de entender la diferencia entre ordenadores programables y cognitivos es con un ejemplo que le dio Darío Gil, vicepresidente de soluciones de IBM a Thomas Friedman y que aparece en su libro ‘Gracias por llegar tarde’¹⁶⁴: Cuando

¹⁶² Recuperado en *El Sesgo Algorítmico y la Protección de Datos Personales* » Torres y Torres Lara - Abogados (tytl.com.pe)

¹⁶³ Recuperado en <https://www.technologyreview.es/s/10924/como-se-produce-el-sesgo-algoritmico-y-por-que-es-tan-difícil-detenerlo>

¹⁶⁴ Friedman, T, *Gracias por llegar tarde*, op. cit.

IBM empezó a desarrollar software de traducción creó un programa para desarrollar un algoritmo que pudiera traducir del inglés al español. Contrataron a lingüistas para que enseñasen a los programadores gramática y, así, entender el lenguaje y poder escribir el programa de traducción. Entonces despidieron a los lingüistas y “cogieron dos textos traducidos por humanos” y los compararon con un enfoque estadístico para saber cuál era el más exacto. Ahora traducen de cualquier idioma a cualquier idioma sin conocerlo. Simplemente facilitan al ordenador multitud de ejemplos de “lo que está bien y de lo que está mal” y da los resultados. El ordenador “nunca tendrá que aprender realmente gramática, ni urdu, ni chino... ¡sólo estadística!

El sesgo algorítmico sucede cuando el sistema de aprendizaje automático refleja los valores de las personas que lo desarrollaron o entrenaron. Por eso es fundamental eliminarlo para poder establecer una legislación con una responsabilidad cuasi objetiva. Es importante señalar que en la actualidad en muchos países de nuestro entorno y también en el nuestro, muchos algoritmos toman decisiones jurídicas y policiales. En 2016, una investigación de ProPublica¹⁶⁵ descubrió que una herramienta de inteligencia artificial utilizada por las fuerzas del orden de USA tenía más probabilidades de declarar que las personas de raza negra corrían un alto riesgo de reincidencia que las personas de raza blanca. El problema radica es que el sistema judicial americano confía en este tipo de herramientas para determinar quién permanece en prisión y quién no. En España el sistema Vigén del Ministerio del Interior toma decisiones en casos de violencia de género para hacer “predicciones de riesgo”.

Bajo la ilusión de que el software no tiene nuestros sesgos, los humanos confiamos en su juicio, ignorando que se han refleja-

¹⁶⁵ <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

do los prejuicios de los creadores. Si aceptamos las decisiones impuestas por la Inteligencia Artificial llegaremos a soluciones sin duda erradas. No podemos permitir que eso ocurra con el uso de los datos de carácter personal. Ahora sí es el momento de la verdad. Lo único que el Estado (o como planteo, una nueva entidad supranacional) debe proteger es la seguridad de las redes de comunicación, el camino por donde pasan nuestros datos y nos protegernos del uso que nosotros, en nuestra propia libertad, les queramos dar.



❖ CAPÍTULO 7. LOS NUEVOS HEREJES: LOS DATOS

Tal y como se señalado los ciudadanos tenemos tres facetas: la pública, la privada y la íntima (o secreta). Las dos primeras son fáciles de conocer y la tercera sólo cuando el individuo la transmite: “*te voy a contar un secreto*”. Esas tres facetas eran claras en el mundo analógico. La transformación digital arrasa con todos esos conceptos.

El informe de Davos señala, también, que “asimismo, la cuarta revolución industrial y el nacimiento de la industria 4.0 se verán auspiciadas, en los próximos años, por las nuevas preocupaciones de los consumidores acerca de los problemas éticos y de privacidad, así como por la longevidad, el envejecimiento poblacional y el aumento de las aspiraciones y del poder económico de las mujeres”¹⁶⁶. Agoreros anuncian la pérdida total de la privacidad (hiperprivacy) y el hipercontrol gubernamental. Son los mismos sesgos con los que nuestros antepasados recibieron a la segunda revolución industrial. Los mismos signos que impidieron a España tomar el tren de la Ilustración. Los mismos mantras que llevaron a Miguel Servet a morir en la hoguera.

Las tres revoluciones industriales que nos han precedido han ayudado a mejorar el mundo. La primera (entre 1760 a 1830) mecanizó la industria con la máquina de vapor; la segunda (1860 a 1914) vino con la electricidad, la producción en masa y la división del trabajo; la tercera (1965 a 1990) la introdujo la informática; desde 2010 transmitamos la cuarta con la interconexión informática e Internet. “Esta cuarta revolución ya

¹⁶⁶ María Jesús Pérez, op. Cit.

nada tiene que ver con planteamientos ideológicos o posiciones políticas, es sencillamente irremediable e irreversible”, sentencia Vidal¹⁶⁷.

Podemos darle vueltas tantas veces como queramos, pero los datos se han convertido en el mayor activo económico del mundo. Vidal explica que la primera internet “la internet técnica” tuvo lugar en el año 93 cuando internet era punto a punto, muy lenta y no se podía distribuir, casi diez años más tarde en el 2002 llegó “la internet empresarial”, la cual ya tenía protocolo e infraestructura y funcionaba de forma distinta, en el año 2008 nació “internet social” por primera vez los usuarios eran capaces de ver cosas en el ordenador que sucedían en un servidor remoto, pero aquí no termina todo ya que en 2014 llegó “internet automático” donde el 97% de las operaciones que hacíamos en el ordenador no las hacíamos nosotros”. Ahora llega el “internet de las cosas”, los objetos empiezan a usar un protocolo propio y comunicarse entre ellos y ya para terminar y este mismo año llegará la era del “internet del todo” cuando se presente el protocolo oficial del 5G. Los aparatos se comunicarán entre ellos.

Como señala Diaz Rojo, “el término privacidad es uno de los más difundidos por los medios de comunicación, así como uno de los más discutidos por los especialistas en temas normativos de la lengua”¹⁶⁸. El problema es que tiende a incorporarse al lenguaje el concepto inglés *privacy*, mucho más amplio que el propio derecho a la intimidad. Por *privacy* se debe entender tanto el derecho a la intimidad, como el derecho al honor y a la propia imagen. A pesar de que recientemente la Real Academia Española haya admitido la palabra *privacidad*, como aquel

¹⁶⁷ Vidal, op. cit. p. 122

¹⁶⁸ Díaz Rojo, JA, *Privacidad: ¿neologismo o barbarismo?*, Espéculo: Revista de Estudios Literarios, Nº. 21, 2002

‘ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión’, la confusión sigue vigente. Pero como señala Díaz Rojo “si a partir del adjetivo *íntimo* se ha creado *intimidad*, no es raro que a partir de *privado* se forme *privacidad*. Las diferencias entre los adjetivos deben trasladarse a los sustantivos correspondientes *intimidad* y *privacidad*. La intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más guardados en el interior -la ideología, la religión o las creencias-, las tendencias personales que afectan a la vida sexual, determinados problemas de salud que deseamos mantener en total secreto, u otras inclinaciones (p. ej., decimos de alguien que «es muy celoso de su intimidad»)»¹⁶⁹. Sin embargo, “Semánticamente, el concepto de *privacidad* no es sinónimo de *intimidad* y *confidencialidad*. La confidencialidad implica el hecho de no dar publicidad o transmitir a terceros datos e informaciones reservadas; la intimidad es lo más interno del sujeto, sus sentimientos y pensamientos profundos; la privacidad está constituida por las facetas que forman nuestra vida personal, frente a nuestra dimensión pública o profesional. Los asuntos íntimos son privados, pero no todos los aspectos privados son íntimos. La residencia personal, las aficiones, las reuniones familiares o la práctica no profesional de un deporte son facetas privadas de un individuo, que forman parte de su privacidad, pero no de su intimidad. Nuestros sentimientos, nuestros miedos, nuestros complejos o nuestras convicciones más profundas constituyen nuestra intimidad, que dado su carácter enteramente personal y particular, son también parte de nuestra privacidad. Por tanto, la privacidad es un concepto más amplio que la intimidad, como reconocen la mayor parte de los juristas. A menudo se emplea incorrectamente *privacidad* en lugar de *intimidad* y *confidencialidad*¹⁷⁰”.

¹⁶⁹ Díaz Rojo, op. cit.

¹⁷⁰ Díaz Rojo, *ibidem*.

El derecho a la privacidad contiene otros derechos autónomos: el derecho a la intimidad, el derecho al honor y el derecho a la propia imagen. El Tribunal Constitucional, a partir de la sentencia 139/2001, de 18 de junio, caracterizó el derecho a la propia imagen como un derecho fundamental autónomo de los demás derechos de la personalidad, y en concreto, del derecho a la intimidad. Afirmó el Tribunal Constitucional en el fundamento cuarto de esta sentencia: «En nuestros anteriores pronunciamientos hemos puesto de manifiesto la vinculación del derecho a la propia imagen con el derecho al honor y con el derecho a la intimidad, pero también hemos señalado que “se trata de un derecho constitucional autónomo que dispone de un ámbito específico de protección frente a reproducciones de la imagen que, afectando a la esfera personal de su titular, no lesionan su buen nombre ni dan a conocer su vida íntima, pretendiendo la salvaguarda de un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás. Por ello atribuye a su titular la facultad para evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual (SSTC 231/1988, FJ 3; 99/1994, de 11 de abril, FJ 5)” (STC 81/2001, FJ 2)».

En una reciente sentencia el Tribunal Constitucional (STC 27/2020) lo deja claro: los medios de comunicación no pueden publicar fotos de las redes sociales sin permiso, a pesar de que el usuario las haya colgado voluntariamente. Para lograr la protección del derecho fundamental a la imagen (uno de los derechos contenidos en la privacidad) para “poder captar, reproducir y/o publicar la imagen de una persona es indispensable su consentimiento inequívoco”. Entre otras cuestiones, porque la

publicación de una fotografía supone una “mayor intromisión en el derecho a la privacidad de la persona”, pues muestra al público sus rasgos haciéndola identificable. El TC reconoce que los sucesos criminales son acontecimientos noticiables, “incluso con independencia del carácter de sujeto privado de la persona afectada por la noticia. Sin embargo, el límite está en la individualización, directa o indirecta, de la víctima, pues este dato no es de interés público porque carece de relevancia para la información que se permite transmitir”.

Veamos entonces cómo afecta a nuestra vida y qué venderemos (o cederemos) y qué no.

La exigencia de privacidad en la era de la individualidad

Parece que privacidad e individualidad sean un mismo concepto, o al menos dos vasos comunicantes que tienden a la igualdad. Pero no lo son.

La vida es una sucesión de renglones torcidos sin esfuerzos. Buscamos atajos y facilidades para transitarla. Hay pastillas para no sufrir. Especialistas en retrasar lo inevitable. Máquinas que nos permiten decir sin oír. Otras que nos permiten ir sin caminar. Peleamos con una PlayStation y viajamos con una televisión. El teléfono es nuestro refugio y nuestra forma de ser, ver, oír y dar. Ese parecer ser nuestro máximo esfuerzo diario. La cultura del esfuerzo ha desaparecido en las nuevas generaciones. “Si me lo hacen para qué esforzarse”, parecen decir nada más despertarse con una alarma que nunca apagan porque pensar en los demás es cansado. La sencillez es un *prius* y el sudor un gesto propio de siglos pasados. Andar es medicinal y el deporte o una forma de vida o algo que hacemos para, posteriormente, disfrutar sin perder la estética con la que nos acercamos al mundo digital.

Con esa forma de vivir es fácil entender que se pida sin dar. Se exija sin ceder. Las nuevas generaciones están en la vida para recibir y no para otorgar. Su hedonismo es tan extremo que no entienden ni siquiera la existencia de un contrato social. Y la exigencia de privacidad es el reflejo de ese nuevo *carpe diem*. Pensamos que es desesperante cuando una web no contesta en milisegundos, dejamos una compra online en cuanto el reloj de arena virtual aparece, repetir un texto, añadir una contraseña memorizada, completar un formulario es cosa del pasado, de la cultura del esfuerzo, de la nemotecnia del teclado con el que necesitábamos diez dedos para escribir. Sí con los pulgares podemos vivir dejemos descansar a los ocho dedos restantes.

Pero olvidamos que todos esos atajos, todos esos renglones que vemos torcidos, falseados por un cerebro cada vez más aletargado, requieren de una máquina que sepa quiénes somos, qué hacemos y qué queremos. Esa máquina necesita datos. Los mismos que hemos cedido para vivir recibiendo. Exigir una vida sin datos es tanto como volver a sudar. Y esa es nuestra propia decisión.

Auguro más sedentarismo, más sencillez, más exigencias y, por tanto, más datos. Cederemos esa parte de nuestro ser a cambio de menos ser y más recibir. Pedir sin dar se puede conseguir en familia. En sociedad, bajo las reglas del contrato social, el egoísmo sólo se materializa a solas, frente al ordenador, con el wifi descargando información a toda velocidad, pero subiendo datos. Subiendo al todo parte de nosotros. Querer otra cosa es, simplemente, vivir en las montañas, sólo y de la caza. Algo a lo que ya no estamos dispuestos a volver. El futuro está aquí. Es más sencillo, menos doloroso y más fácil. Todo gracias a los datos y a la paradoja de Pulgarcito.

La paradoja de Pulgarcito

Nos levantamos por la mañana y empezamos a generar datos; existen en todo lo que usamos o hacemos. Teléfonos, coches, electricidad, comprar, etc. Todo está controlado por datos o, a su vez, genera datos. Los datos son migajas digitales con los que podemos medir e identificar el comportamiento de la sociedad. Por eso lo he llamado Síndrome de Pulgarcito. En el famoso cuento infantil, Pulgarcito deja migas de pan para saber volver a casa y un gigante se las come. En Internet pasa algo parecido con las cookies, unos pequeños archivos que nos identifican para facilitarnos volver a la misma información que vimos. A su vez, ese rastro o huella digital nos detecta y permite realizar un patrón de conducta que unido a otros configuran nuestra propia identidad digital.

En este contexto, señala el profesor Morales García, “la eclosión tecnológica que nos ha envuelto a todos se está convirtiendo en nuestra peor pesadilla. Toda nuestra vida volcada sobre la red, almacenada y espiada por los poderes públicos para la prevención del delito”¹⁷¹. Una asfixia, señala con acierto el profesor Óscar Morales, que “hace irrespirable cualquier atmósfera de libertad” porque lo mismo que tememos es lo que nos ayuda. Ahí radica la incongruencia. Lo mismo que nos ayuda nos desprotege (incongruencia de inteligencia). El equipo del MIT Media Lab, capitaneado por Sandy Pentland, estudia el patrón de interacción de las personas en comunidad y es capaz de saber cómo un grupo se relaciona, además de medir su índice de pobreza analizando el “patrón de interacciones” a través de cómo usan los coches o con qué bicicletas circulan. Pues bien, imaginemos las redes sociales, un elemento de macrodatos que

¹⁷¹ Morales García, O, *El control informático de la libertad (o la crónica de una muerte anunciada)*, en VVAA, Ruiz Rodríguez, L, *Respuestas Internacionales a los retos de la seguridad*, pp. 215-228, Tirant Lo Blanc, 2009.

permite determinar comportamientos, tendencias y mucha otra información. Cada minuto se envían 204 millones de correos electrónicos, se cuelgan 275.000 tweets y 200 millones de post de Instagram.

Para algunos, como el doctor en informática Pablo Rodríguez, estos rastros digitales contienen nuestra “alma”. “Son un espejo de ti mismo”. Considera que los datos pueden revelar nuestro lado emocional, convirtiéndolos en los nuevos psicólogos, en un “nuevo coach”. Añade: “internet ha hecho que dispongamos de datos en abundancia, que estén por todas partes y que sean mucho más valiosos. Tanto si sales a correr como si ves la tele o simplemente estás senado en el coche en un atasco, prácticamente cada actividad que desarrollas crea un rastro digital, más materia prima para las destilerías de registros”¹⁷² que con inteligencia artificial sacan un “valor añadido” a esos datos.

Rodríguez es la voz de muchos otros tecnoagoreros. Sin embargo, el propio autor realiza un análisis más realista cuando señala que los cambios tecnológicos nos permitirán vivir de un modo mucho más eficiente si conseguimos que “ellos” (los datos) no nos dominen a “nosotros”. Otorgar a los datos la capacidad de humanizarse es el problema del discurso tecnócrata. Más si se confiere a un código binario la capacidad de tener o contener “alma”. Como ya he dicho, los datos por sí solos no significan nada y para que sean útiles deben ser compilados y analizados. Y parte del problema es el error semántico, ya comentado, entre privacidad e intimidad.

El alma, en cambio, en un todo en sí mismo. Sin entrar en sus diferentes acepciones con la existencia de un alma nos referimos a los seres humanos o, al menos, a los seres vivos en gene-

¹⁷² Rodríguez, P, *Inteligencia Artificial*, op. cit.

ral. Por tanto, nuestros rastros digitales no pueden contener nuestra alma como personas. A pesar de ello, como se verá, sí creo que en veinte años los humanos tendremos una especie de dualismo antropológico descrito por Platón: una analógica, similar a la actual y otra digital. La personalidad digital será el compendio de nuestros datos, algo que *strictu sensu* no contendrá alma, aunque sí corresponderá a una realidad material de nuestro comportamiento digital. No estaremos ante nada parecido al alma ya que esos datos carecerán de expectativa razonable de privacidad por cuanto, como se verá, serán datos negociables, transmitibles y con valor económico. Hablamos de rastros que por voluntad propia cederemos a cambio de esa vida digital.

Que un ciudadano registre cada una de las acciones que realiza, tanto despierto como dormido, ha dejado de ser el rasgo distintivo de un personaje *cyberpunk* creado por William Gibson para convertirse en un hombre de carne y datos. Se llama Chris Dancy y se presenta como speaker con la rotundidad de esta afirmación: “Internet ha muerto, larga vida a la Inner-Net”, señala Dancy en su propia web. Él es el hombre más conectado del mundo. “Todos sus movimientos, temperatura corporal, presión sanguínea, oxígeno y peso están digitalizados. También la calidad del aire que respira, el volumen de su voz, los alimentos que ingiere, la temperatura ambiente, la humedad, la luz, el sonido o todo lo que mira en televisión, entre otras muchas cosas”, señala la BBC¹⁷³. Dancy tiene once dispositivos en su cuerpo y cientos de aparatos en su casa de Brentwood -una pequeña localidad en Tennessee, EE.UU.- que le ayudan a cuantificar y registrar todo lo que hace y a medir sus constantes vitales a diario.

¹⁷³ <https://www.bbc.com/mundo/noticias-39668781>

Controlar sus datos vitales constantemente le ha permitido dejar de fumar, perder peso y llevar una dieta más saludable. Sin embargo, ni siquiera sus rastros no permitirían conocer su alma. Pero los datos son lo que nos permitirá en el futuro conocernos mejor. El Mit Lab ha medido la segregación en diez ciudades norteamericanas con datos de móviles. Han examinado a qué locales va la gente durante el día. A cada usuario le han asignado una renta según el lugar donde pasaba las noches. Por tanto, cada punto está anonimizado, pero tiene asignada una renta por su barrio. ¿Qué han encontrado?, señala El País que: “la mitad de la segregación que hay en EEUU se debe a tus elecciones cotidianas. Cuando vas a comer, entras en un lugar que tiene gente como tú y no gente distinta de ti”, explica Pentland. La obligación de un ayuntamiento es buscar espacios donde ciudadanos de rentas dispares se encuentren. En Riad (Arabia Saudí), encontraron que la mayoría de afectados por paro crónico vivía en zonas donde el transporte público era malo”¹⁷⁴.

La paradoja de la incongruencia digital

“La importancia de la revolución de los datos es como la electricidad o la imprenta”, dice Alex Sandy Pentland, cofundador del MIT Media Lab y uno de los siete científicos de datos más destacados del mundo, según Forbes. “Ha cambiado completamente el mundo, más que cualquier tecnología del siglo XX”, añade¹⁷⁵. Del MIT Media Lab han salido las pantallas táctiles, la tinta electrónica, el GPS y otras creaciones que han transformado el mundo. Innovación y disrupción bajo el lema de “conectar la tecnología con lo humano para afrontar los grandes retos”. Este reconocidísimo laboratorio multidisciplinar (o ‘an-

¹⁷⁴ https://elpais.com/tecnologia/2019/11/18/actualidad/1574108885_423569.html

¹⁷⁵ El País. 19.11.2019

tidisciplinar’, como ellos dicen) ha sido el caldo de cultivo para el progreso tecnológico los últimos 30 años, señala un estudio de Innovación¹⁷⁶.

Como ya he señalado el equipo de MIT Media Lab examina el patrón de interacción en comunidades para “comprender la esencia de una comunidad”, características sociales que hasta hoy eran “imposibles de cuantificar”. Se mide el patrón de las comunidades porque “no es la tecnología lo que dicta la esencia”, son las personas y las ideas que fluyen entre las personas o que diferencia a “una comunidad de otra”. Sin embargo, serán los propios datos los que nos permitan conocer si el contrato social está agotado y de ahí el contrasentido o la paradoja. Señala Portland que a través de la IA y la ciencia de los datos podremos ver que “los patrones de la comunicación son, aparentemente, el factor más importante a la hora de determinar las características humanas de una comunidad. Según parece no es el nivel de educación lo que más importa, ni tampoco el marco regulatorio: son las interacciones humanas”¹⁷⁷. Antes de disponer de estos estudios no se entendía por qué había delincuencia en unos lugares y en otros no. “Hasta que empezamos a disponer de unas miguitas digitales que nos han permitido analizar los patrones reales de interacción”, señala Sandy Portland.

La comunicación social es la que nos dirá si se debe cambiar o no el contrato social. Paradójicamente son los propios datos los que nos ayudarán a entenderlo y, es por ello, que son tan importantes. Tanto que la Asamblea General de las Naciones Unidas obliga a los ciento noventa y tres países miembros que midan los datos “para el bien social”. Los datos son, por tanto, un bien social que debe ser explotado, aunque como veremos en

¹⁷⁶ <https://innovadores.larazon.es/es/investigacion-en-espanol-en-el-mit-media-lab/>

¹⁷⁷ Prólogo a la edición de Inteligencia Artificial de Pablo Rodríguez, op. cit.

este trabajo con diversos límites. La ONU señala que “promover el uso de los datos con fines positivos” debe ayudar a “comprendernos mejor a nosotros mismos, comprender a nuestras comunidades y ayudar al mundo en general”. Son un nuevo bien personal en la búsqueda de un bien social.

En este sentido el Instituto Nacional de Estadística de España puso en 2019 un experimento que tuvo mucha polémica: el análisis de millones de teléfonos para saber cómo se mueven los consumidores o conocer el historial de navegación les sirve para averiguar comportamientos. El tratamiento de todos estos nuevos datos para el bien común es lo que Pentland lleva estudiando una década. “Tenemos que integrar los datos en el contrato social”, dice Pentland. “Sabemos cómo manejar el dinero, cómo manejar la tierra, pero cómo manejaremos los datos es un reto enorme”, sentencia¹⁷⁸.

Pentland, cuyos trabajos están en el origen del Reglamento General de Protección de Datos de la UE señala que la visión ciudadana de los datos es errónea. Un informe del 15 de noviembre de Pew Research en Estados Unidos reveló que un 81% del público cree que los riesgos de la recolección de datos por parte de las empresas superan sus ventajas y el 66% dice lo mismo del Gobierno. Las cifras reflejan una preocupación creciente pero mal entendida. “No reúnas todos tus datos en un sitio, que es lo que como humanos tendemos a hacer, sino dejémoslos donde se recogen y enviemos preguntas pre acordadas”, explica a El País. Los algoritmos que analicen esos datos deben ser abiertos y revisables: “Si eres una teleco, te voy a mandar el algoritmo 23, lo pasas por tus datos y cuelgas la respuesta en abierto”, explica. Sin embargo, la descentralización

¹⁷⁸ Por qué los experimentos con datos de móviles son inevitables y buenos para la sociedad | Tecnología | EL PAÍS (elpais.com)

de datos por la que abogado (no reunir todo en un mismo sitio) es la protección que todos debemos tomar en la actualidad. En una regulación de caja fuerte digital de datos todos estarían en un mismo sitio porque no se protegerá el dato en sí, sino la cápsula que los protege. Como he dicho es más importante regular la seguridad de los datos que los datos en sí mismo.

El control ciudadano y la transparencia deberán presidir un nuevo contrato social, tal y como indica Pentland. Sin embargo, a diferencia de él, considero que deberán ser un control centralizado y controlado por el ciudadano en el contrato social de su personalidad digital.

El data driven: los datos en el centro de la empresa

Marc Vidal señala que “el futuro no es de los digitalizados sino de los transformados”¹⁷⁹. Y para transformarnos debemos:

- Incorporar el internet de las cosas
- Socializar la oferta centrada en el cliente
- Saber gestionar los datos en *big data*

El hombre (el cliente) es el centro de los negocios. Pero no olvidemos que es un hombre encerrado en su habitación con un mando a distancia (el teléfono) con el que controla, compara y compra. En poco tiempo y a solas puede saber más que años antes en una reunión de briefing colectiva. Conoce la oferta y la adapta a su propia demanda. El teléfono sabe lo que quiere y se lo presenta. Él compara, elige, pregunta y al momento tiene una oferta adaptada a sus necesidades. Él es el centro de la cadena de valor. El consultor en estrategia y doctor en ingeniería industrial Gustavo Mata señala que “cualquier bien material, servicio o

¹⁷⁹ Vidal, M., op. cit.

idea no es realmente un producto si no es para la satisfacción de una necesidad; el producto es casi un accidente en la satisfacción de la necesidad: lo trascendental es el cliente y su necesidad”¹⁸⁰.

Conocer al cliente y sus necesidades permite satisfacerlas. Así es cómo se vende en el presente y cómo se venderá en el futuro. Y eso solo se podrá conseguir conociendo los datos del cliente y que éste conozca los de las empresas. Recoger, procesar, limpiar y visualizar los datos será una parte más de la cadena de negocio para contentar al consumidor final. Las estadísticas son claras¹⁸¹:

1. La experiencia del cliente superará al precio y al producto como el diferenciador clave de la marca. (Walkerinfo)
2. Las empresas de EE. UU. pierden aproximadamente 83 mil millones de dólares en ventas al año debido a la mala experiencia de los clientes. (CustomerExperienceBoard)
3. El 91% de los clientes insatisfechos no harán negocios con una marca que no cumplió con sus expectativas. (CustomerThink)
4. Los clientes leales valen aproximadamente 10 veces el valor de su primer pedido. (CustomerThink)
5. Los departamentos de marketing en grandes empresas usan un promedio de 65 aplicaciones diferentes. (Forbes)
6. El 80% de los datos de los clientes se desperdiciarán debido la mala gestión de los datos en las “cadenas de valor”. (CustomerExperienceBoard).

Pero los clientes tienen miedo al uso que la empresa haga de sus datos. Es cierto la evolución trae riesgos. ¿Se negociará con datos? Sí, como en la actualidad ya se hace. Lo que Snowden nos hizo conocer posiblemente se incrementará, pero el deseo de

¹⁸⁰ Mata, G., Un nuevo modelo para la cadena de valor, recuperado en Microsoft Word - apuntes de estrategia y competencia.doc (gustavomata.com)

¹⁸¹ Recuperado en <https://landings.powerdata.es/ebook-como-instaurar-una-cultura-data-driven-en-mi-empresa>

control de los Gobiernos siempre ha existido. La seguridad forma parte del mismo contrato social y la pérdida de libertad (discriminación) nunca será tal como la que existió de forma previa a la Ilustración. Es cierto, se debe legislar para proteger, igual que se hará con el derecho robótico. Los humanoides deberán ser regulados, así como los riesgos asociados a la robótica. Pero no podemos exigir evolución, no podemos mirar al futuro y que nuestros sesgos mentales nos impidan evolucionar.

Si se incrementan las penas asociadas a los delitos que genere el *big data* acabaremos con un sistema punitivo de la Ilustración. Reclamar una *hiperprivacy* sin entender que el uso de las tecnologías de la información exige que nuestra expectativa de privacidad decaiga es no entender el contrato social o intentar impedir que el futuro llegue.

Entre la protección europea y la desprotección China, Estados Unidos nos adelantará. Europa con sus regulaciones de la *hiperprivacy* impide una evolución a la que se aboca china a cambio de azúcar. La decisión está en nuestros políticos: evolución o protección. Creo que la evolución sin sobreprotección es el término medio al que nos debemos abocar. La nueva directora del CNI dijo en su toma de posesión que nuestros servicios de inteligencia se están digitalizando. Sus hombres y mujeres saben que si quieren ganar la guerra al terrorismo deben acceder a sus medios tecnológicos. Nuestro teléfono móvil sabe más de nosotros que nuestros seres queridos. Ahí está lo público, lo privado y lo secreto. Y nuestros espías se preparan para protegernos. Lo harán, como hasta ahora, con el marchamo de la protección de las garantías constitucionales de los ciudadanos que da un magistrado del Tribunal Supremo. Yo no quiero Guantánamos en nuestro país, pero tampoco más ataques terroristas como el de Atocha. Y en el análisis de datos está nuestra protección como Estado Nación.

El internet de las cosas (IDC): la integridad y seguridad es más importante que la privacidad

Es el futuro. Futuro que sin datos no existirá. La Internet de las Cosas (Idc) es “la interconexión a través de Internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos”¹⁸². Unos chavales cansados de ir a comprobar si la máquina de Coca Cola tenía producto la conectaron a la red. Buscando la comodidad encontraron el futuro. Los aparatos se conectan con aparatos. Miles de millones de dispositivos físicos en todo el mundo que ahora están conectados, recolectando y compartiendo datos¹⁸³. Por tanto, el problema no es tanto la privacidad sino la seguridad. El libro “*Click here to kill everybody*”¹⁸⁴ lo deja claro: no es tan preocupante la actividad como que alguien pueda cambiar nuestra ficha médica, el tipo de sangre, a lista de alergias o que ataque un fibrilador.

La integridad y la seguridad de los datos es más importante que la privacidad, como lo fue la integridad personal en el primer contrato social. Señala Rodríguez que los dispositivos inteligentes como los electrodomésticos, las prendas de vestir o los coches “revelan información más específica sobre nuestra conducta”¹⁸⁵ que el smartphone. Y a ellos se lanzarán los hackers. Rodríguez cree que para vulnerar nuestros datos personales. Sin embargo, para convertir eso en un negocio debería ser un hackeo masivo. El problema, por tanto, debe centrarse en la seguridad y no en el objetivo que buscan los hackers. ¿Por qué?

¹⁸² Digitaltrends, recuperado en ¿Qué es el Internet de las Cosas? Todo lo que necesitas saber sobre IoT | Digital Trends Español

¹⁸³ <https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/>

¹⁸⁴ Schneier, B, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W. Norton & Company; Reprint edición, 2018.

¹⁸⁵ Rodríguez, op. Cit.

Porque los sistemas de seguridad funcionan bajo el principio de Pareto, también conocido como la regla del 80-20. Establecida por el economista Wilfredo Pareto observó que el 20% de la población poseía el 80% de la riqueza. A lo largo de su estudio comprobó que esta relación porcentual se repetía en diversos grupos y distribuciones en la vida real. Según este principio el 80% de los riesgos podrán ser controlados con el 20% de los controles de seguridad. Así, la revista Cuadernos de Seguridad señala que “bajo el Principio de Pareto consideramos que el 20% de las causas son las que provocan el 80% de los problemas, es decir, si solucionamos el 20% de las causas críticas, se resuelven el 80% de los problemas existentes, por el contrario, si actuásemos sobre el 80% restante de las causas «triviales», únicamente lograríamos reducir la totalidad de los problemas en un 20%.”¹⁸⁶

Por tanto, hay un 20% desprotegido algo que utilizan los hackers para atacarnos. Algo que nos permite crecer en el Idc con rapidez, pero sin seguridad. En cambio, dicho principio no se aplica a la privacidad.

El caso Carpenter: el cambio de paradigma internacional

El 22 de junio de 2018, la Corte Suprema de los EE. UU. emitió una decisión en *Carpenter vs. Estados Unidos*, sosteniendo que el gobierno federal necesita una orden para acceder a los registros de ubicación de teléfonos móviles.

Vayamos al caso: un hombre estaba involucrado en robos a mano armada en el área de Detroit. El Ministerio Fiscal centró la prueba en cargos en los registros telefónicos. El FBI había obtenido la información en virtud de la Ley de comunicaciones

¹⁸⁶ Pascual, O, El principio de Pareto en la gestión del riesgo patrimonial, Cuadernos de Seguridad, 2019.

almacenadas (SCA) que establece que el gobierno puede exigir la divulgación de registros de telecomunicaciones cuando “hechos específicos y articulables muestran que hay motivos razonables para creer que el contenido de una comunicación electrónica o electrónica, o los registros u otra información buscada, son relevantes y materiales para una investigación criminal en curso “. Este estándar SCA no requiere una orden judicial y es inferior al estándar aplicado bajo la Cuarta Enmienda, que requiere una orden judicial cuando un individuo demuestra una expectativa legítima de privacidad. En la decisión, el Tribunal acordó que debería existir un estándar más alto para acceder a los registros de localización de los teléfonos móviles debido a su naturaleza intrusiva de los mismos.

Durante décadas, el Tribunal Supremo de Estados Unidos había sostenido reiteradamente que las personas no tienen una expectativa razonable de privacidad en los registros en poder de terceros proveedores de servicios porque las personas proporcionan voluntariamente su información a terceros. Bajo ese estándar, el gobierno y las fuerzas del orden tenían permitido realizar búsquedas sin orden de datos de ubicación de teléfonos móviles. Es decir, como Movistar (un tercero) conoce mi posición es innecesaria la orden judicial. El Gobierno, sabedor de que un cambio de paradigma afectaría a las investigaciones prospectivas policiales¹⁸⁷, argumentó que las personas no tienen una expectativa legítima de privacidad en los registros de los teléfonos celulares. El gobierno citó la doctrina de terceros, que representa el principio de que cualquier información que se brinde voluntariamente a terceros no puede mantener una expectativa razonable de privacidad.

¹⁸⁷ Para más información del caso *Carpenter*, vid. Villegas, MA, *La sentencia Carpenter v. United States: ¿La primera gran victoria de la privacidad en la era digital?*, Diario La Ley, N° 9316, 2018

El Supremo sentenció que las personas tienen una expectativa legítima de privacidad en los registros de ubicación de sus teléfonos móviles. La decisión *Carpenter* se ha convertido en una desviación de décadas de jurisprudencia, que anteriormente sostenía que proporcionar voluntariamente su información a un tercero era una pérdida de una expectativa legítima de privacidad, como en el caso de 1979 de *Smith v. Maryland*, donde la Corte Suprema dictaminó que un robo.

“El mapeo de la ubicación de un teléfono celular en el transcurso de ciento veintisiete días proporciona un registro completo del paradero del titular”, escribió el presidente del tribunal Roberts en la opinión de la mayoría, citando una opinión anterior. “Al igual que con la información de GPS, los datos con marca de tiempo proporcionan una ventana íntima a la vida de una persona, revelando no solo sus movimientos particulares, sino también a través de ellos sus” asociaciones familiares, políticas, profesionales, religiosas y sexuales “. La posición adoptada por el Tribunal reconoce la creciente prevalencia de la tecnología en la vida diaria y la dependencia de las personas de ella.

“Ninguna doctrina constitucional debería presumir”, decía el informe, “que los consumidores asumen el riesgo de vigilancia gubernamental sin orden judicial simplemente mediante el uso de tecnologías que son beneficiosas y cada vez más integradas en la vida moderna”. Además, con esta decisión, el Tribunal reconoce que a medida que nuestras vidas se registran cada vez más en línea, las expectativas en torno a esos espacios están cambiando. “Muchas personas esperan que las protecciones otorgadas a su hogar y efectos personales se extiendan a su ser digital”, señala la sentencia que determina, de golpe, la validación de la protección constitucional de la identidad digital y del entorno digital.

En Europa el golpe sobre la mesa lo dio el Tribunal de Justicia de la UE al considerar que Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, suponía “una injerencia de gran magnitud y especial gravedad” en los derechos fundamentales a la privacidad y a la protección de datos. El Tribunal de Justicia señaló, en primer lugar, que los datos que han de conservarse permiten saber con qué persona y de qué modo se ha comunicado un abonado o un usuario registrado, determinar el momento de la comunicación y el lugar desde el que ésta se ha producido y conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto. “Estos datos, considerados en su conjunto, pueden proporcionar indicaciones muy precisas sobre la vida privada de las personas cuyos datos se conservan, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados”, señaló el fallo¹⁸⁸.

“Al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes -prosigue el Tribunal-, la directiva se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal”. “Además, el hecho de que la conservación y la utilización posterior de los datos se efectúen sin que el abonado o el usuario registrado sea informado de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante”, resaltó el fallo a pesar de que admite que la conser-

¹⁸⁸ Recuperado de El TJUE anula la Directiva que obligaba a la conservación de los datos de los usuarios de servicios de comunicaciones electrónicas · Noticias Jurídicas (juridicas.com)

vación de los datos “responde efectivamente a un objetivo de interés general, a saber, la lucha contra la delincuencia grave y, en definitiva, la seguridad pública”. Sin embargo, estima que se han sobrepasado los límites que exige el respeto del principio de proporcionalidad.

En segundo lugar, la directiva “no fija ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes únicamente tendrán acceso a los datos y podrán utilizarlos para prevenir, detectar o reprimir penalmente delitos que, por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia”. En particular, el acceso a los datos no se supedita al control previo de un órgano jurisdiccional o de un organismo administrativo autónomo.

En tercer lugar, añade, en lo que atañe al período de conservación de los datos, la norma prescribe un período de entre seis y dos años sin precisar “los criterios objetivos con arreglo a los que debe determinarse el período de conservación para garantizar que se limite a lo estrictamente necesario”. El Tribunal de Justicia considera asimismo que la directiva no contiene garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de los datos. “En particular, autoriza a los proveedores de servicios a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican (especialmente en lo que respecta a los costes de aplicación de las medidas de seguridad) y no garantiza la destrucción definitiva de los datos al término de su período de conservación”, señala el fallo.

El caso *Carpenter* en USA y la sentencia del TJUE señalan un cambio en la forma de considerar al ciudadano y su control.

Pero el Presidente del Tribunal Supremo también dijo que las técnicas de recolección que involucran asuntos exteriores o seguridad nacional no se consideran en esta decisión y que se harán excepciones para emergencias como amenazas de bomba y secuestro de niños donde los derechos de privacidad de las personas se considerarán contra el interés de proteger a las personas contra daños inminentes, o destrucción inminente de evidencia. Es así, en derecho la doctrina Pareto no es aplicable. Es cierto, la cesión de datos a terceros no genera una falta de expectativa razonable si los terceros implementan medidas de seguridad para proteger los datos. Las compañías de telefonía protegen estos datos que no son públicos y, por ende, están sujetos a la protección del derecho. ¿Ocurre lo mismo si la cesión es a una plataforma pública como Facebook o Twitter? Veámoslo.

Hacia la protección del entorno digital y no de la persona analógica

Tradicionalmente en nuestro país se venía considerando que en el registro de dispositivos o sistemas informáticos podían verse comprometidos dos diferentes derechos fundamentales, a saber: el derecho a la intimidad del usuario del dispositivo, ya que todos los datos que es posible almacenar en el mismo son susceptibles de «afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc.» (STC 173/2011, de 7 de noviembre) y al derecho fundamental al secreto de las comunicaciones si el registro del dispositivo alcanzaba a datos almacenados que formaran parte de procesos comunicativos.

La solución al problema provocó lo que hoy se conoce como “derecho al entorno virtual” cuyo antecedente jurisprudencial

se establece en la STC 173/2011, de 7 de noviembre cuando señala: «quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona».

Esta doctrina se vio reflejada en las medidas de investigación tecnológica a las que la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal establece para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica de la LECrim. El punto de partida de esta regulación y que da sentido a la misma aparece recogido en el Preámbulo de la Ley 13/2015, cuando descarta que los dispositivos de almacenamiento masivo de información puedan ser considerados como simples piezas de convicción. Su capacidad para recoger y conservar datos de muy diferente índole permite que el acceso a los mismos pueda llegar a afectar de manera intensa a diversos derechos fundamentales y, de ahí, la naturaleza y exigencias de la regulación legal. Esta idea, ya reconocida por la jurisprudencia, deriva de la consideración de los ordenadores como algo más que un instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad del usuario (STS n.º 342/2013, de 17 de abril).

La LECrim viene, por tanto, a dar solución a lo que nuestros tribunales venían reclamando. Así lo reconocía la STS 342/2013, de 17 de abril, cuando señalaba que en el derecho al entorno virtual se integraría «sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris pro-

pio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos». Esta resolución pone de relieve «la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital».

Esta nueva línea jurisprudencial se acerca, por tanto, a la doctrina que emana del caso *Carpenter*. En nuestro país ya no se proteger la intervención de un teléfono celular por el derecho al secreto en las comunicaciones sino la personalidad digital y su entorno virtual. Así se señala que: “En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar -de hecho, normalmente albergará- información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones” (STS 311/2020).

Es, por tanto, ese entorno digital, al que he venido denominando la “caja fuerte de datos” el centro de cualquier modificación y el núcleo de protección que únicamente mediante consentimiento limitado podremos ir concediendo. En algunos casos el consentimiento será tácito (frente a Hacienda para realizar nuestras declaraciones de la renta) y otros expreso (frente a Google para que pueda utilizar nuestros datos). El Estado será el garante de la seguridad de que las redes de comunicación sean seguras y nosotros seremos el único garante frente a nuestra propia caja fuerte digital. Pero antes debemos desterrar miedos y sesgos.



❖ CAPÍTULO 8. ¿HEMOS ACEPTADO SER ESPIADOS?

Hoy en día las redes sociales forman parte de nuestra vida. También los asistentes de voz virtuales, los gps o los relojes de pulsera inteligentes. En todos los casos su uso requiere que aceptemos, de forma previa, su política de protección de datos desconociendo el uso que de los mismos hace la red social¹⁸⁹.

Según un informe publicado por la Universidad del Noreste de los Estados Unidos¹⁹⁰, los altavoces inteligentes se activan y nos escuchan una media de diecinueve veces al día. Alexa, Siri, Cortana o el Asistente de Google, graban lo que les rodea cuando escuchan palabras que suenan similares a las fórmulas con las que estos se activan, como por ejemplo: “Oye, Siri” o “Alexa” o “Ok, Google”. Y en todos los casos hemos aceptado que lo hagan simplemente con ponerlos en marcha.

Google ha admitido que “expertos del lenguaje” contratados por la firma escuchan aproximadamente el 0,2% de las conversaciones que los usuarios mantienen con su asistente virtual, lo que implica que una parte de esas interacciones no son privadas. Amazon, Samsung y Apple, además de Google, asumen que las conversaciones entre un usuario y su asistente son del todo privadas y que la interacción se produce exclusivamente mediante inteligencia artificial, es decir, que los únicos que “es-

¹⁸⁹ Un estudio de la Universidad Carlos III de Madrid elaborado por José González Cabañas, Ángel Cuevas y Rubén Cuevas revela que Facebook utiliza información sensible de los usuarios con fines comerciales. Lo más preocupante es que, según la estimación de los autores del estudio, el 73% de los usuarios de Facebook están etiquetados con alguna información sensible, lo que supone aproximadamente el 40% de la población de toda la Unión Europea.

¹⁹⁰ <https://moniotrlab.ccis.neu.edu/smart-speakers-study/>

cuchan” al usuario son robots. Pero ahí aparece otro sesgo: la creencia de que nos espían.

“¿Quién ha visto un aviso, que le haya hecho pensar que su micrófono está escuchando sus conversaciones?”, empieza preguntando un profesor a sus alumnos en el documental *Gran Hacked*, disponible en Netflix. Todos levantan la mano, ríen, y él sigue: “Los anuncios que parecen increíblemente precisos, que nos hacen pensar que nos espían, muy probablemente sean la prueba de que el targeting funciona y que predice nuestra conducta”¹⁹¹. El Targeting tiene como objetivo alinear la publicidad a las necesidades de los clientes a los que se quiere llegar. Los analiza, sabe lo que les interesa y les planta la publicidad en su próxima búsqueda por Internet. Luego usaremos Google para comparar y aparecerán las mejores ofertas. Google es nuestro verificador de hechos, es decir, se ha convertido en profesor, prescriptor y vendedor.

“Cualquier aplicación que uno instala en el teléfono recibe por parte del usuario ciertos permisos. Algunas necesitan usar el micrófono o la cámara (WhatsApp o Instagram no podrían funcionar sin ellos) para traficar audios, fotos o videos. Si bien esto es legítimo, también es cierto que ese micrófono o esa cámara pueden ser usados más allá del fin específico con que se autorizó. A veces pareciera, aunque no está probado, que ese micrófono está escuchando y usando Inteligencia Artificial (IA) para detectar un interés puntual”, dice Andrés Piazza, consultor y especialista en regulación de Internet¹⁹².

Señala Villarde “la red nos genera la ilusión de que en realidad la comunicación activa o pasiva que establecemos a través suyo

¹⁹¹ Citado en Espionaje tecnológico: entre lo ilegal y lo ilegítimo | Perfil

¹⁹² <https://www.perfil.com/noticias/cordoba/espionaje-tecnologico-entre-lo-ilegal-y-lo-ilegitimo.phtml>

es opaca al mundo, no deja rastro; es un proceso de comunicación solo aparentemente libre, abierto y público. Esa aparente opacidad nos estimula a ser menos prudentes con nuestra privacidad en la falsa creencia que estamos a salvo de la mirada ajena. El precio que se paga por hacer uso ilimitado de semejante fuente inagotable e inabarcable de información que es la red es la fragilidad de nuestra vida privada¹⁹³. Sin embargo, esta visión choca frontalmente con las estadísticas internacionales sobre la percepción del anonimato en Internet. En el mismo sentido que Villarde señala Goodnow: “*We definitely do not take online privacy seriously enough*”¹⁹⁴.

Recientemente el Tribunal Constitucional (STC 27/2020) lo ha dejado claro. En el caso concreto de Facebook, el Constitucional destaca que no puede obviarse que la información ofrecida en esta red social está inmersa en “una maraña de cláusulas contractuales contenidas en un prolijo y extenso documento alojadas en lugares del sitio web de difícil acceso para el usuario, reservándose, por otro lado, la plataforma la posibilidad de modificar las condiciones de uso y privacidad en cualquier momento, sin necesidad de preaviso a los usuarios registrados que con anterioridad las hubieran aceptado”. Por tanto, la Sala entiende que “hay que concluir que el ciudadano desconoce el contenido real y las consecuencias del otorgamiento de la autorización exigida para su registro y utilización, pues resultan de difícil comprensión para cualquier usuario medio que no disponga de conocimientos jurídicos y tecnológicos, por lo que difícilmente en este caso puede hablarse de un consentimiento basado en información fiable o confiable”.

¹⁹³ Villaverde I, La intimidación, ese “terrible derecho” en la era de la confusa publicidad virtual, *España Jurídica: Journal of Law*, Vol. 14, N.º. 3, 2013, págs. 57-72.

¹⁹⁴ Recuperado en *The Dangers of a Digital Age: Are We Taking Online Privacy Seriously Enough?* | Rasmussen University

¿Qué ha pasado? “Es innegable”, dice el Tribunal, que “algunos contornos de los derechos fundamentales al honor, a la intimidad y a la propia imagen pueden “quedar desdibujados” y que “la utilización masificada de estas tecnologías de la información añade nuevos problemas jurídicos a los ya tradicionales. Si bien es un hecho que el funcionamiento de las redes sociales permite la difusión de información personal, también lo es que puede significar una pérdida de control de la información suministrada por el propio usuario”. En ese sentido, el tribunal advierte “por obvio que resulte” de que “los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica”. Lo he dicho, pero es fundamental repetirlo: el reconocimiento constitucional de los derechos fundamentales comprendidos en el artículo 18 de la Constitución conlleva la potestad de la persona de controlar los datos que circulan en la red social.

El problema radica en que las concepciones de público y privado han cambiado. “Los usuarios han pasado de una etapa en la que eran considerados meros consumidores de contenidos creados por terceros, a otra -la actual- en la que los contenidos son producidos por ellos mismos. Con plataformas como Facebook, Twitter, Instagram o Tuenti los usuarios se han convertido en sujetos colaborativos, ciudadanos que interactúan y que ponen en común en redes de confianza lo que tienen, lo que saben o lo que hacen, y que comparten con un grupo más o menos numeroso de destinatarios -usuarios igualmente de la Red Social- todo tipo de imágenes, información, datos y opiniones, ya sean propios o ajenos”, explican el TC.

Tal y como señala el catedrático Villarde “el proceso de comunicación pública sobre el que se asienta el entramado de libertades constitucionales pertenecientes al grupo de los derechos de interrelación con otros (libertades de expresión, informa-

ción, derecho a la información, honor, intimidad y propia imagen, protección de datos, reunión y manifestación y asociación), ha sido un espacio físico y real de comunicación interpersonal (la plaza pública, la calle, los medios de comunicación...) era un espacio definido físicamente, bien por el espacio en el que tenía lugar el proceso de comunicación (la plaza pública...), bien por el soporte en el que éste se producía (la prensa...) hasta la irrupción del empleo de internet como un foro público de comunicación interindividual mediante redes sociales y otros medios de difusión de opiniones e información imaginables (lo blogs puede ser el ejemplo conspicuo)¹⁹⁵.

El Supremo considera que: “El derecho a la intimidad personal y familiar garantiza a la persona un ámbito reservado de su vida personal y familiar, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean estos poderes públicos o particulares. Este derecho atribuye a su titular el poder de resguardar ese ámbito reservado, tanto personal como familiar, frente a la divulgación de este por terceros y frente a la publicidad no consentida. Así lo ha declarado tanto el Tribunal Constitucional (entre las más recientes, sentencia 176/2013, de 21 de octubre) y esta sala (sentencia 478/2014, de 2 de octubre)”.

El Tribunal Supremo asienta que “el consentimiento del titular de la imagen para que el público en general, o un determinado número de personas, pueda ver su fotografía en un blog o en una cuenta abierta en la web de una red social no conlleva la autorización para hacer uso de esa fotografía y publicarla o divulgarla de una forma distinta, pues no constituye el «consen-

¹⁹⁵ Para un análisis del proceso de comunicación pública véase cualquiera de los trabajos de Ignacio Villaverde Menéndez, tanto sus libros *Derecho a ser informado. Estado democrático e información*, Junta General del Principado de Asturias, Oviedo 1994, *Los derechos del público*, Tecnos, Madrid, 1995; y finalmente su *Los derechos del público: la revisión de los modelos clásicos de “proceso de comunicación pública”*, Revista española de derecho constitucional

timiento expreso» que prevé el art. 2.2 de la Ley Orgánica 1/1982 como excluyente de la ilicitud de la captación, reproducción o publicación de la imagen de una persona. Aunque este precepto legal, en la interpretación dada por la jurisprudencia, no requiere que sea un consentimiento formal (por ejemplo, dado por escrito), sí exige que se trate de un consentimiento inequívoco, como el que se deduce de actos o conductas de inequívoca significación, no ambiguas ni dudosas.”

La teoría de la “integridad contextual”

En el pasado las comunidades eran pequeñas e íntimas. La información personal se preservaba en la memoria de la familia. Hoy el modelo de difusión de la información no es a través de la boca a la oreja sino del “lenguaje de la electricidad”, donde la información se desliza en código binario. En este sentido, todos podemos escaparnos del control de la comunidad liberándonos “de las normas sociales que inhiben la individualidad y la creatividad”. En el lado negativo, se crea una serie cada vez mayor de registros sobre casi todas las facetas de la vida de una persona. A medida que las empresas y el gobierno comparten cada vez más información personal, se reúnen “expedientes digitales” sobre casi todas las personas¹⁹⁶.

Desde las primeras concepciones de privacidad defendidas por John Stuart Mill hasta la actualidad la protección de la vida privada se ha centrado en la distinción entre lo público y lo privado. El espacio público es aquel constituido por los asuntos que incumben a la colectividad y donde la necesidad de la interacción supone un todo. Por otro lado, lo privado es lo reservado del individuo, esto es, “su esfera protegida o aquella donde

¹⁹⁶ Daniel Solove. The digital person. Technology and Privacy in the Information Age, recuperado en The Digital Person: Technology and Privacy in the Information Age (core.ac.uk)

se desarrollaba su intimidad y vida privada”. Dicha consideración presupone para Noain Sánchez que, “dado que lo propio de la esfera reservada del individuo es, por esencia, su intimidad y vida privada, esta carecerá de protección en el momento que salga a la arena pública”¹⁹⁷.

“Cuando compro en la droguería, lo hago a la vista del público, la persona que realiza el pago ve lo que estoy comprando. Pero eso no significa que el contenido de compra, ya sean las vitaminas, los tintes para el cabello o la salud sexual, deba transmitirse a todos en la tienda, o compartirse con mis estudiantes, o incluso con mi familia. Aquí, la privacidad no se trata de una noción absoluta de secreto de la información privada frente a la pública. Se trata del reconocimiento de que, en ciertos contextos, se divulgan ciertas piezas de información, y las normas, ya sean sociales, legales o estructurales, rigen el flujo de información personal dentro de ese contexto particular”¹⁹⁸. Por tanto, como señala David Lyon, los ordenadores «no han creado la situación en la que los ciudadanos de las sociedades avanzadas se encuentran actualmente. Éramos súbditos de los datos mucho antes de que se produjera ninguna supuesta revolución”¹⁹⁹. Lo que sí es novedoso es la capacidad de análisis de la información.

La evolución nos conduce a pensar que la dicotomía público-privado ya no existe en nuestra personalidad digital. Hoy cedemos esa intimidad para poder realizar acciones tan cotidianas como pagar con tarjeta de crédito o ir al médico. La consecuencia es la capacidad de control sobre el individuo en su faceta pública. La profesora de ciencias de la información Hellen Nissenbaum es la precursora del estudio de la indefinición de

¹⁹⁷ Amaya Noain Sánchez. La protección de la intimidad y vida privada en internet

¹⁹⁸ Michael Zimmer. Privacy and Surveillance in Web 2.0: A study in Contextual Integrity, and the Emergence of “Netaveillance”

¹⁹⁹ Lyon, D. (1995): El ojo electrónico

ambas esferas. Para verificar la ineficiencia del modelo bipolar privado versus público, Nissenbaum “parte del análisis de tres principios que han guiado las políticas de protección de la vida privada en la tradición jurídica anglosajona, tres formas de conceptualizar la privacidad por oposiciones entre binomios: competencias gubernamentales para vigilancia y control de datos versus privacidad del individuo, designación de lugares públicos frente a lugares privados o espacios de no intromisión y catalogación entre información sensible e información no sensible. Dichas oposiciones, aunque útiles desde perspectivas teóricas, conllevan carencias por cuanto la aplicación de estos principios no es siempre obvia y en numerosas ocasiones, la línea divisoria no es ni estática, ni universal”²⁰⁰.

Lo que describe Zimmer es la teoría de la privacidad desarrollada por Helen Nissenbaum llamada “integridad contextual”. Un reconocimiento clave dentro de la integridad contextual es que la multitud de actividades de intercambio de información tienen lugar en una “pluralidad de ámbitos distintos”. Dentro de cada uno de estos contextos, existen normas, ya sea implícita o explícitamente, que dan forma y limitan nuestros roles, comportamientos y expectativas. La teoría de la integridad contextual se basa en la noción de que “no hay arenas de la vida que no estén gobernadas por normas de información”. Estas normas explican los límites de nuestros derechos subyacentes con respecto a la información personal, y nuestra privacidad se invade cuando se infringen las normas informativas.

Ya no existen recetas generales. Para determinar si se ha mantenido la integridad contextual, debemos considerar cómo la nueva tecnología o práctica afecta a todos los agentes involucrados: personas, Gobiernos y empresas. Se debe examinar: la

²⁰⁰ Citado en Noain Sánchez, La privacidad como integridad contextual y su aplicación a las redes sociales

idoneidad y el tipo de información, la transparencia y la privacidad. Estando de acuerdo con la integridad contextual, considero que sería mucho más efectivo que existiesen dos tipos de personalidad. La analógico con una ley común y la digital donde entran en contexto todos los agentes involucrados.

Nuestra morada informática

En este sentido, si permitimos que los datos los almacene el propio usuario en su caja de seguridad desde un punto de vista punitivo la protección, y por tanto la garantía, debe centrarse en el acceso ilícito. Como bien señala la doctrina, por todos, Morales García, “Por ello, tal vez sea conveniente formular un concepto de domicilio informático²⁰¹, del derecho a mantener la máquina y su contenido al margen de los accesos no deseados, tal como sucede, *ceteris paribus*, con el domicilio “físico”; concepto, pues, en el que integrar los elementos esenciales de bienes jurídicos con relevancia constitucional, directamente ligados al uso de la tecnología (en el caso del Derecho español, huelgan los comentarios en relación con la ubicación sistemática, el art. 18 CE, de la cláusula de tutela frente a los peligros de la informática), describiendo con ello un tipo de carácter objetivo, en los términos recomendados por la Convención, con la pretensión de salvaguardar la esfera íntima del sujeto y sin desdeñar una protección escalonada a través de la creación de subtipos agravados”.

En cualquier caso, señala el autor, “debe tenerse en cuenta que la creación de tipos penales con finalidades trascendentes, de resultado cortado, como sucede con el 197.1 segundo inciso en el CP español de 1995, donde se condiciona la punición de la intercep-

²⁰¹ No entramos a exponer el debate que actualmente existe en la doctrina penal acerca del bien jurídico en el delito de intrusismo informático, ni la errónea ubicación de este delito entre los delitos contra la intimidad, remitiéndonos para las distintas posiciones mantenidas por los autores acerca del bien jurídico, si es la intimidad, el domicilio informático o la seguridad informática, a: Carrasco Andrino, M. del M., El delito de acceso ilícito a los sistemas informáticos

tación de las comunicaciones (o en el 197.2 CP, de la interceptación de datos) a la finalidad de conocer la intimidad o los secretos, solo puede perturbar la aplicación ordinaria del tipo, de modo que la prueba de dicha finalidad sucesiva, (que ni siquiera debe realizarse en un resultado sino simplemente inspirar la conducta principal de acceso o interceptación) será poco menos que imposible, permaneciendo en la impunidad la mayoría de accesos ilegales. La creación de subtipos agravados, además de reforzar la tutela de los bienes jurídicos en juego, permitiría mantener la punición del tipo básico cuando los elementos del agravado no concurrieren o no pudieran ser objeto de prueba en el plenario”²⁰².

“El ordenador comporta hoy día un nuevo espacio en el que desarrollar nuestra vida personal, constituyendo una especie de «morada informática» en la medida en que en él se realiza y a él va a para una buena parte de nuestra actividad cotidiana, de manera que los datos e informaciones contenidas, programas manejados, etc., pueden permitir a quien acceda a ellos, adentrarse en un espacio de desarrollo personal, de ejercicio de libertad”, señala Morales García²⁰³. Es lo que he venido definiendo como “entorno digital”.

Sobre este particular Morales Prats²⁰⁴ acierta cuando afirma que el acceso a los datos de un ordenador es una forma de “control certero, sistemático, penetrante e invisible sobre la persona”,

²⁰² Morales García, O, Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convección del consejo de Europa sobre Cyber-Crime, Cuadernos de derecho judicial, Nº. 9, 2002 (Ejemplar dedicado a: Delincuencia informática : problemas de responsabilidad / Oscar Morales García (dir.)), págs. 11-34

²⁰³ Sobre esta reclamación de la consideración del ordenador como una «morada informática o domicilio informático», Morales García, O.: «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre el Cibercrimen», Delincuencia Informática. Problemas de Responsabilidad, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002,

²⁰⁴ Morales Prats, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”.

pues subrayan de manera precisa el carácter lesivo de la intimidad de las conductas de intromisión en un ordenador y contacto con todo aquello que en él se archiva y resguarda de intromisiones no consentidas. Mediante ese acceso se pueden descubrir facetas de la personalidad del individuo que, aisladamente consideradas pueden carecer de significado intrínseco, pero que, si fueran enlazadas entre sí, “arrojarían como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado”.²⁰⁵

Establecido, por tanto, que el bien jurídico a proteger es la privacidad como contenedor de otros derechos, toca determinar qué significa privacidad.

El efecto spillover en los datos

El esfuerzo por aceptar que algo nuevo y “fuera de lo común” es algo muy estudiado en nuestra psique. Sí somos refractarios hacia lo inesperado, más si es complejo. Pero es una realidad de nuestro tiempo: a más complejidad más renuencia. Pero intentemos entender qué ocurre con nuestros datos.

En teoría del crecimiento económico se entiende por *knowledge spillover* el [efecto] desbordamiento del conocimiento. La imagen es clara: “una empresa innovadora desarrolla conocimientos, pero esos conocimientos no quedan confinados en la propia empresa, sino que desbordan o rebosan sus límites y pasan a ser, aunque no lo quiera y sin que pueda evitarlo, de dominio público, de manera que otras empresas pueden aprovecharlos. [...] No conviene traducir este término simplemente como «transferencia del conocimiento» (knowledge transfer), ya que

²⁰⁵ Sánchez Carazo, C.: La intimidad y el secreto médico, Díaz de Santos, Madrid, 2000, pág. 16, haciéndose eco de las palabras de la Exposición de Motivos de la anterior Ley Orgánica 5/1992, de 29 de octubre, de tratamiento automatizado de datos de carácter personal

esta se distingue del «desbordamiento del conocimiento» en que es intencionada. Spillover a secas podría traducirse como «efecto desbordamiento», «efecto derramamiento» (muchísimo menos utilizado), «externalidad» o sencillamente «efecto indirecto»²⁰⁶. Pues bien, algo así pasa con los datos en cuanto salen de nuestra individualidad.

Déjenme poner un ejemplo. Para cada uno la receta de la tortilla de patatas de nuestras madres es la mejor. Ellas (algunas, la mía no) eliminan algún ingrediente para que nadie les pueda copiar. Pero con la receta casi completa a base de prueba y error conseguiremos completarla. Así son los datos. A pesar de que salgan anonimizados podremos completar el cuadro. Si yo sé que Juan nació en Barcelona en una fecha determinada, aunque no sepa su apellido si tengo acceso al censo sabré cuántos Juanes nacieron en un día determinado en Barcelona. Encontrando otros datos acabaré poniendo nombre a Juan. O peor. La ONU necesita datos para realizar pronósticos acerca de los problemas que podría enfrentar la humanidad dentro de algunos años, y por eso lanzó una herramienta interactiva denominada population.io, que recopila información acerca de los índices de natalidad a nivel mundial. El sitio permite saber cuántas personas nacieron en el mismo día que uno, en qué países están, cuántas son mayores y menores y en qué fecha próxima uno se convierte en un habitante estadísticamente importante como, por ejemplo, ser el humano número 5 mil millones en la Tierra. Así son los datos y su efecto spillover. Y lo peor es que los datos no se evaporan.

Pues bien, los datos son una masa grasienta que se cuela por las rendijas y que, a pesar de ser anónima, se puede llegar a identificar. La pregunta es: ¿hasta qué punto lo sabemos y lo aceptamos?

²⁰⁶ Unidad *c.es*.3, DGT, Comisión Europea, recuperado en [puntoycoma n.º 97 \(europa.eu\)](http://puntoycoma.n.º97.europa.eu)

La identidad digital

El concepto de identidad digital se utiliza para intentar resolver estos problemas. Por ejemplo, las Naciones Unidas han propuesto utilizarlo para ayudar a los refugiados, que constituyen una parte sustancial de la población indocumentada. “Queremos que cada refugiado tenga una identidad digital única”, declaró Filippo Grandi, alto comisionado de la ONU para los refugiados, en octubre de 2017. “Esto mejorará la rendición de cuentas y facilitará la comunicación bidireccional entre los refugiados y los proveedores de servicios. También ayudará a prevenir y reducir la apatridia”²⁰⁷.

Siguiendo al World Economic Forum, en palabras de Chomsky, la identidad de una persona está integrada por atributos, es decir por elementos o características sobre aquella. Los atributos pueden ser agrupados en tres grandes categorías: (i) inherentes, que son aquellos cuyo origen está en la persona y no depende de ningún factor exterior a la misma; (ii) acumulados, que son aquellos que el sujeto o individuo tiene a partir de sus decisiones personales y respecto de los cuales tiene, en principio, pleno control; y (iii) asignados, que son aquellos que el individuo obtiene a partir de su interacción con terceros y sirven para denotar cierta relación que la persona ha establecido en su vida.²⁰⁸

Daniel Buchner, director de programas de la División de Identidad de Microsoft explicó que: «Esto coloca a los proveedores de identidad en un lugar de control, entre nosotros y cada interacción digital en nuestras vidas. Nuestro objetivo es crear un ecosistema de identidad descentralizado en el que millones de

²⁰⁷ Recuperado en Identidad Descentralizada: Cómo Microsoft (entre otros) planean capacitar a los usuarios para administrar y controlar datos personales (cointelegraph.com)

²⁰⁸ World Economic Forum, «A Blueprint for Digital Identity», Future of Financial Services Series, agosto de 2016

organizaciones, miles de millones de personas e innumerables dispositivos puedan interactuar de forma segura a través de un sistema interoperable basado en estándares y componentes de código abierto»²⁰⁹.

Por tanto, en la dicotomía que defiende de identidad analógica y digital debemos entender que en la analógica nuestra personalidad está centralizada y en la digital existe tal descentralización como programas y redes de comunicación necesitamos para vivir. Un médico requerirá las redes de consulta y de estudio médico. Los profesionales que han desarrollado las vacunas covid han confiado en redes especializadas de intercambio de datos. Su personalidad digital profesional las requería, aunque la privada navegase por Google preguntando dónde comprar una pizza mientras trabajaba. Por tanto, en una vida digital descentralizada son muchos los elementos que pueden establecer cuál es nuestra personalidad digital y cuáles son los patrones de modulación del consentimiento informado. Esos médicos querían que las redes que usaban para enviar datos y muestras del covid fuesen seguros y los compartían en estados embrionarios para asegurarse de que las agencias del medicamento lo autorizasen de forma veloz. Primaron la velocidad a cambio de seguridad. Volvemos por tanto al ejemplo de las tarjetas de crédito. Pero a su vez se desprotegían al navegar en la búsqueda de comida o de un regalo para su marido o mujer. Y esos datos son tan valiosos como los de la vacuna del covid.

Pagar al ciudadano por el uso de sus datos. A eso acabaremos reduciendo el acceso a la caja de seguridad de datos. Como se ha dicho los datos son petróleo y tienen un valor económico. En España podemos entender que el derecho a la privacidad en

²⁰⁹ <https://es.cointelegraph.com/news/decentralized-identity-how-microsoft-and-others-plan-to-empower-users-to-own-and-control-personal-data>

su faceta de exclusión está protegido constitucionalmente, aunque se puedan ceder los derechos. En este sentido, la STS 754/2008, establece que “se produce en el supuesto una cuestión relativa a la vertiente de explotación comercial de la imagen que carece de dimensión constitucional y se concentra en el ámbito del contrato. No niega la Sala que se haya vulnerado el derecho a la imagen de la recurrente por la empresa de cosméticos, lo que se considera es que ésta no lo ha hecho al concurrir la cesión expresa efectuada por quien aparecía como titular de la imagen reproducida, lo que creó una apariencia en la que confió de que quien le estaba cediendo los derechos era titular de los mismos”.

La doctrina del TC, en su respectivo ámbito de competencia, ha venido distinguiendo, sin embargo, el contenido o aspecto constitucional del derecho y su contenido o aspecto comercial o patrimonial, al que se refiere, precisamente, el artículo 7.6 de la O 1/1982. En la STC 81/2001, de 26 de marzo, se declara que “como ya se apuntó en la STC 231/1988, F. 3 y, sobre todo, en la STC 99/1994, el derecho constitucional a la propia imagen no se confunde con el derecho de toda persona a la explotación económica, comercial o publicitaria de su propia imagen, aunque obviamente la explotación comercial incontestada -e incluso, en determinadas circunstancias, la consentida- de la imagen de una persona puede afectar a su derecho fundamental a la propia imagen”.

La protección de los valores económicos, patrimoniales o comerciales de la imagen afecta a bienes jurídicos distintos de los que son propios de un derecho de la personalidad, y por ello, aunque dignos de protección y efectivamente protegidos, no forman parte del contenido del derecho fundamental a la propia imagen del art. 18.1 CE. Dicho en otras palabras, a pesar de la creciente patrimonialización de la imagen y de la «necesaria

protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma» (STC 170/1987, de 30 de octubre), el derecho garantizado en el artículo 18.1 CE, por su carácter «personalísimo» (STC 231/1988, F. 3), limita su protección a la imagen como elemento de la esfera personal del sujeto, en cuanto factor imprescindible para su propio reconocimiento como individuo.

Por su parte, la STC 156/2001, de 2 de julio, declaró que “la protección constitucional de este derecho no alcanza su esfera patrimonial, ya que el conjunto de derechos relativos a la explotación comercial de la imagen, aunque son dignos de protección - y en nuestro Ordenamiento se encuentran protegidos, en especial en la LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y a la propia imagen-, no forman parte del contenido del derecho fundamental a la propia imagen que consagra el art. 18 CE”.



❖ CAPÍTULO 9. PROTEGER NUESTROS DATOS: HACIA LA TRANSPARENCIA

Tal y como he establecido en los diversos trabajos que he realizado sobre el derecho a la intimidad este derecho se concibe en su origen como un derecho al aislamiento y a la soledad. Era el derecho a la intimidad de la era predigital. La sociedad del siglo XIX y de principios del siglo XX clamaba para que el Estado no interfiriese en su vida. En 1890 los abogados Samuel Warren y Louis Brandeis publican el artículo *The right to privacy*²¹⁰ en la revista Harvard Law Review. En su escrito realizan una adaptación del concepto jurídico establecido años años por el juez Cooley: *the right to be let alone* que se fundamenta en el principio básico heredado del derecho inglés: *a man's house as his own castle or my home is my castle*.

Este derecho nace sin antecedentes normativos a causa de un conflicto personal del propio Samuel Warren. Él y su mujer realizaban fiestas sociales que eran ampliamente criticadas por la prensa de la época. Warren tomó medidas y configuró este derecho para evitar la intromisión en lo que ocurría dentro de su vivienda. La intimidad predigital busca, por tanto, la protección del individuo de forma negativa reconociéndole facultades de exclusión sobre un ámbito determinado: su casa. La sociedad del siglo XIX y de principios del siglo XX clamaba porque el Estado no interfiriese en su vida privada. Este derecho nace sin antecedentes normativos a causa de un conflicto personal, el del propio Warren. Posteriormente amplía las áreas de exclusión: su propio cuerpo, el domicilio, el correo o el teléfono. Tal

²¹⁰ Samuel D. Warren; Louis D. Brandeis, *The right to privacy*, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220

y como se señala la doctrina²¹¹ la intimidad física “refleja una concepción territorial de la intimidad en cuanto que circunscribe el objeto de protección a espacios o zonas que quiere mantener oculto y reservado”: el secreto como bien jurídico protegido.

Sin embargo, al compás del desarrollo tecnológico la intimidad, como derecho negativo, da paso a una nueva realidad, la autodeterminación informativa. El objeto de protección se traslada a tener una facultad positiva (control) y una negativa (exclusión) de su propio derecho a la intimidad. La concepción tradicional del derecho a la intimidad protege espacios y realidades físicas centrado en un derecho que introduje en mi tesis doctoral y que hoy está ampliamente aceptado por los tribunales: la expectativa razonable de intimidad.

El derecho a la intimidad en la era de internet: la privacidad

Tal y como señala López Ortega “reducir la tutela de la intimidad a su dimensión territorial, prescindiendo del contenido informativo del derecho, supone ignorar que las intromisiones más graves y penetrantes, las que se producen en un contexto tecnológico, conciernen a la vertiente informativa de la intimidad. Lo que la revolución tecnológica ha propiciado es que injerencias mínimas, incluso banales en la intimidad física, potencien sus efectos invasivos por la cantidad y la calidad de las informaciones que pueden llegar proporcionar. La prueba de ADN constituye un buen ejemplo de una injerencia de escasa intensidad en la intimidad corporal que, sin embargo, es capaz de producir una injerencia especialmente intensa en el ámbito informativo (perfil genético)”²¹².

²¹¹ Por todos, López Ortega, JJ, El derecho a la intimidad: nuevos y viejos debates, Dykinson, 2017.

²¹² López Ortega, JJ, op. Cit.

Con el desarrollo tecnológico la defensa de la intimidad se centra en la protección de los datos de carácter personal. “A la inviolabilidad del cuerpo, el domicilio o las comunicaciones como mecanismos de defensa de la intimidad territorial, se suma desde finales del pasado siglo la potestad del ciudadano para controlar el uso de sus datos personales por parte de terceros a través del reconocimiento de su derecho a la autodeterminación informativa. Este derecho, que opera como cimiento axiológico sobre el que se asienta la disciplina conocida como «protección de datos», pese a ser concebido como independiente y autónomo por la jurisprudencia constitucional, ha definido la principal línea de defensa de la intimidad informativa desarrollada hasta la fecha”²¹³.

Por tanto, en una sociedad interconectada como la que viene, la tutela del derecho a la intimidad, articulada en torno a la idea de autonomía individual, se desvirtúa en pos de una protección de la autodeterminación informativa. La primera referencia a dicho concepto surge de la Sentencia de 15 de diciembre de 1983 dictada por el Tribunal Constitucional Federal de Alemania (TCFA) en relación con la ley del censo²¹⁴ que declaró la inconstitucionalidad de dicha norma en virtud de la excesiva cantidad de información personal que se requería al ciudadano para, con posterioridad, someterla a tratamiento informatizado. En la actualidad, que no decir de la revolución que viene con el Internet de las cosas, desde el nacimiento y la configuración de nuestra personalidad jurídica no es posible sustraerse al control de los datos salvo que pretendamos convertirnos en anacoretas y parias sociales. Por tanto los conceptos tradicionales de protección son inoperantes. Por eso es tan necesaria una nueva regulación adap-

²¹³ López Ortega, JJ y Alcoceba Gil, JM, “De la intimidad territorial a la informativa: la defensa de la intimidad a través de sus manifestaciones constitucionales”

²¹⁴ Daranas, «Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la personalidad y dignidad humana», Boletín de Jurisprudencia Constitucional, núm. 3, 1984.

tada a los tiempos que nos protejan del control estatal y del control de las grandes corporaciones que manejan nuestra libertad de movimientos en las redes de comunicación.

“La solución más obvia a la cuestión planteada parece ser la transmutación en espacios íntegramente virtuales de la intimidad como derecho al anonimato, al olvido, o, en esencia, en la capacidad de determinar cómo, cuándo y en qué medida se genera información susceptible de ser conocida por otros, así como hasta qué momento esa información debe ser accesible para los demás”, señala López Ortega. Veamos si es posible.

Hacia una gestión de la confianza y no de la intimidad

En la obra *Privacy and Freedom*, el profesor Alan Westin establece que los seres humanos no deseamos ni el aislamiento completo ni la sobreexposición. “Para vivir y prosperar, los seres humanos necesitamos de condiciones intermedias”, señala²¹⁵. Por ello, el profesor Morales Prats establece el concepto de balanceo de derechos. Todos los derechos tienen anti derecho, salvo el derecho a la vida porque, como regla general, no existe el derecho a la muerte. En consecuencia, Westin definió el derecho a la privacidad como el derecho a controlar la información personal de cada uno. Las legislaciones modernas en materia de privacidad se basan en gran medida esta forma de entender el derecho: dar a las personas el control sobre su información personal.

Los tecnólogos, ajenos a las concepciones generales del derecho, han adoptado la tragedia de los comunes y la han llevado a su discurso sobre el habeas data. “La privacidad del consumidor también es un recurso escaso que sufre la tragedia de

²¹⁵ Westin A, *Privacy and Freedom*, IG Pub, 2015.

los bienes comunes. Impulsadas por los ingresos publicitarios, las corporaciones se tornan cada vez más eficientes en la recopilación y el uso de datos del consumidor para dar forma su comportamiento²¹⁶. Los impuestos y las regulaciones son la solución más conocida para la tragedia del problema de los bienes comunes. El Reglamento Europeo de Protección de Datos Personales es un claro ejemplo hacia dónde estamos caminando.

Tal y como ya he señalado, en España el discurso se ha mantenido por autores como González siguiendo a Nikolaos Laoutaris que en su artículo *Cows, Privacy, and Tragedy of the Commons on the Web*²¹⁷, establece una analogía clara con la parábola neomaltusiana. El punto principal de su enfoque es que si los modelos de negocio (agricultores) y las tecnologías (vacas) consumen la confianza del usuario (pasto) más rápido que su tasa de reposición (servicios gratuitos que nos hacen felices), en algún momento la confianza se dañará más allá reparación y los usuarios simplemente abandonarán la web, algo que de por sí parece inviable.

Esta visión simplista bebe del estudio de los profesores de derecho Joshua Fairfield y Christoph Engel que deconstruye el enfoque clásico de la privacidad al señalar que cuando una persona elige revelar información personal, el acto con frecuencia también revela los datos personales de otros. Así, señalan que cuando una empresa analiza los datos una embarazada y los compara con listados públicos de nacimientos puede determinar cuáles de las mujeres que compraron en sus tiendas estaban embarazadas en el momento de la compra y qué elementos eran los más idóneos para ofertar. En este sentido Fairfield y

²¹⁶ <https://steemit.com/blockchain/@bornswift/data-privacy-and-the-tragedy-of-the-commons>

²¹⁷ Lauotaris, op. cit.

Engel consideran que la cesión de datos privados afecta a terceros en sus bienes comunes. “El control individual de los datos es un concepto fundamentalmente defectuoso²¹⁸”, señalan.

Usan la tragedia de los comunes para poner sobre el tapete que la privacidad debe ser un bien público. “Desde una perspectiva individual, por lo tanto, tiene sentido continuar compartiendo la información. Pero si todos tomamos esta decisión, como todos lo haremos, esto terminará creando una sociedad agotada en la privacidad en la que pocos desean vivir”, señalan los autores. Lo llaman la “paradoja de la privacidad”, en la que las personas dicen en las encuestas que no quieren revelar su información personal a otros, pero en la práctica lo hacen sistemáticamente afectando al derecho de sus conciudadanos.

Los autores apuntan, como otros han señalado, hacia una especie de sindicato de datos, al estilo de los sindicatos que permitieron los avances en materia laboral, obviando, al estilo neomaltusiano, que el análisis de datos producirá una evolución social mucho más beneficiosa que perniciosa. “Tal como lo describen, la divulgación de información de un individuo sobre sí mismo y los demás contribuye a la falta general de privacidad en la cultura. El individuo sufre el costo de vivir en esa cultura. Esta lesión es la misma que sufre cualquier otro miembro del público. Además, la divulgación de información por parte del individuo no restringe ni la suya ni la capacidad de otra persona de revelar información y utilizar el recurso de privacidad en el futuro”²¹⁹.

²¹⁸ Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*

²¹⁹ Dennis Hirsch. *Privacy, Public Goods and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 *Duke Law Journal Online* 67 (2016), Ohio State Public Law Working Paper No. 347

Tal y como señalan Richards & Woodrow Hartzog²²⁰, la economía de la información se basa en el intercambio de información personal; está “mediado por relaciones de información” en mucho mayor medida que las economías anteriores. En idéntico sentido Hirsch señala que “participar en la economía de la información en consecuencia requiere que confiemos en otros con nuestra información personal. Este tipo particular de confianza, “confianza digital”, consiste en nuestra fe de que los proveedores de bienes y servicios digitales utilizarán nuestra información personal para beneficiarnos, no perjudicarnos”²²¹.

Es cierto, la economía de la información depende de la confianza digital. Si las personas se convencieran de que los motores de búsqueda, los sitios de redes sociales, los sitios web y otros proveedores de este tipo estaban utilizando su información personal para perjudicarlos, compartirían menos. Por ejemplo, los investigadores del MIT y Digital Fourth descubrieron que, a raíz de las revelaciones de Snowden, las búsquedas de Google en términos controvertidos disminuyeron. Un estudio del 2016 del Centro de Investigación Pew, que consta de una encuesta y grupos focales, concluyó que la voluntad de los estadounidenses de compartir información personal con entidades comerciales era “contingente” sobre si los beneficios de hacerlo superaban los riesgos de privacidad y seguridad²²².

Los encargados de formular políticas y las partes interesadas han luchado durante años sobre si la autorregulación de la industria o la regulación directa del gobierno protegerían de manera más efectiva y eficiente la información personal del abu-

²²⁰ Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law* recuperado en Microsoft Word - 19-3-2-richards-hartzog-final.docx (stanford.edu)

²²¹ Dennis Hirsch, *op. cit.*

²²² Lee Rainie & Maeve Duggan, *Pew Research Ctr., Privacy and Information Sharing* recuperado en PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf (pewresearch.org)

so²²³. Sin embargo, considero que la mejor forma de trabajar en este sentido es con la creación de un sistema descentralizado y personal donde nuestra identidad analógica tenga un control sobre la identidad digital. Descentralizando y personalizando el control de los datos personales, el individuo decidirá en qué momento y con quién compartir los datos de su identidad digital. Lo que pretendo es que el culmen de la autodeterminación de los datos, el verdadero liberalismo económico de nueva vida digital.

El sesgo del desdoblamiento

George Orwell acuñó el término “no persona” en su novela distópica 1984 e introdujo el concepto de Gran Hermano, que todo lo ve y controla. Advierte de los peligros de la concentración del poder y de la manipulación de la verdad, exterminando el pasado y el pensamiento libre. “Quien controla el pasado, controla el presente, quien controla el presente controla el futuro.”. El término «orwelliano» se ha convertido en sinónimo de las sociedades totalitarias y represoras. Algunos creen que algo así puede ocurrir en el futuro.

El usuario Deepfakes publicó en la red social Reddit los resultados de un programa de inteligencia artificial que reemplazaba, de forma realista, los rostros de unas personas por otras. Hoy manipular vídeos e implantar la cara de personas es posible. Según el Wall Street la inteligencia artificial basada en algoritmos de aprendizaje conseguirá crear vídeos que no levanten sospechas sobre su falso contenido entre la mayoría de las personas. Las fake news darán un paso más y se pueden llegar a convertir en la muerte de la verdad. Y nosotros somos los trans-

²²³ Cary Coglianese & David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, recuperado en Management-Based Regulation: Prescribing Private Management to Achieve Public Goals - Coglianese - 2003 - Law & Society Review - Wiley Online Library

misores de estas noticias. Somos nosotros quienes las convertimos en virales. Nuestra mente juega en nuestra contra al creer nos algo que no existe debido a lo que los señores de la psique denominan disonancia cognitiva.

La disonancia cognitiva es un concepto muy conocido en la psicología que supone el autoengaño de los humanos. Cuando una idea entra en conflicto con una de nuestras creencias. El concepto fue formulado por primera vez en 1957 por el psicólogo estadounidense Leon Festinger, en su obra *A Theory of Cognitive Dissonance*²²⁴. La teoría de Festinger plantea que, al producirse esa incongruencia o disonancia de manera muy apreciable, la persona se ve automáticamente motivada para esforzarse en generar ideas y creencias nuevas para reducir la tensión hasta conseguir que el conjunto de sus ideas y actitudes encajen entre sí, constituyendo una cierta coherencia interna²²⁵. Por eso, La percepción de la IA y la informática cognitiva está muy lejos de la realidad (Friedman).

Manipulamos nuestras propias ideas para dar importancia a nuestra creencia del pasado. El sesgo de confirmación es uno de esos elementos que nos lleva a descartar ideas provocadoras por el simple hecho de serlo. La noción de sesgo cognitivo, como ya se ha dicho, fue introducida por Daniel Kahneman y Amos Tversky en 1972, y surgió de su experiencia con la imposibilidad de las personas de razonar intuitivamente con órdenes de magnitud muy grandes, o anumerismo (*innumeracy* en inglés). El lingüista Noam Chomsky estable que “en un estado totalitario no importa lo que la gente piensa, puesto que el gobierno puede controlarla por la fuerza empleando porras. Pero cuando no se puede controlar a la gente por la fuerza, uno tiene que

²²⁴ Festinger, L., *A Theory of Cognitive Dissonance*, Stanford University Press, 1957.

²²⁵ https://es.wikipedia.org/wiki/Disonancia_cognitiva

controlar lo que la gente piensa, y el medio típico para hacerlo es mediante la propaganda (manufactura del consenso, creación de ilusiones necesarias), marginalizando al público en general o reduciéndolo a alguna forma de apatía”²²⁶. Sin embargo, en democracia, el sistema de manipulación es diferente.

Señala Chomsky que en un mundo en el que “la riqueza está concentrada y en el que existen grandes conflictos de intereses de clase, el cumplimiento de tal papel requiere una propaganda sistemática”²²⁷ (Chomsky y Herman). Chomsky y Herman describen los filtros a los que se recurre a partir de la clasificación de la información que se considera apta o no apta para la audiencia.” “La democracia participativa presupone la capacidad de la gente normal para unir sus limitados recursos, para formar y desarrollar ideas y programas, incluirlos en la agenda política y actuar en su apoyo. En ausencia de recursos y estructuras organizativas que hagan posible esta actividad, la democracia se limita a la opción de escoger entre varios candidatos que representan los intereses de uno u otro grupo que tiene una base de poder independiente, localizada por lo general en la economía privada.”²²⁸

Chomsky, en cambio, no es el autor de “las diez estrategias de manipulación mediática”, texto que se ha convertido en un fenómeno viral en Internet. El verdadero autor es el francés Sylvain Timsit. El documento fue publicado por primera vez en francés, en 2002, con el título original “Stratégies de manipulation”, en la web syti.net. Según el francés se nos manipula haciéndonos creer que el Estado nos conoce mejor que nosotros mismos. “Gracias a la biología, la neurobiología y la psico-

²²⁶ Chomsky, N citado en Manipulación mediática según Noam Chomsky - Wikiwand

²²⁷ Chomsky y Edward S. Herman en Manufacturing Consent. The Political Economy of the Mass Media, vintage Digital, 2010.

²²⁸ Chomsky op cit.

logía aplicada, el “sistema” ha disfrutado de un conocimiento avanzado del ser humano, tanto de forma física como psicológicamente. El sistema ha conseguido conocer mejor al individuo común de lo que él se conoce a sí mismo. Esto significa que, en la mayoría de los casos, el sistema ejerce un control mayor y un gran poder sobre los individuos, mayor que el de los individuos sobre sí mismos”. Por eso es tan importante para el Sistema controlar nuestros datos en internet y, por eso, es fundamental que podamos reconducir el contrato social.

La creación de perfiles de identidades personales y las decisiones automatizadas plantean importantes riesgos para los derechos y libertades. “Estos procesos pueden ser opacos. Puede que las personas no sean conscientes de que se está creando un perfil sobre ellas o que no entiendan lo que implica. La elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren. Esto puede socavar su libertad a la hora de elegir, por ejemplo, ciertos productos o servicios como libros, música o noticias. En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada”²²⁹.

Estos sesgos y miedos parece que nos alejen de nuestro futuro. Pero, además, existe en la actualidad una especie de nuevo sesgo cognitivo, la del desdoblamiento, algo que deberá estudiar la psicología. Estamos viviendo una doble vida, la digital y la analógica. En la analógica nuestra imagen es peor que en la digital donde nos esforzamos en parecer lo que, en realidad, no somos. Nace la persona digital y los dosieres digitales. Solove señala que a medida que los datos fluyen nacen los dosieres

²²⁹ <https://www.enfoquederecho.com/2019/11/07/el-sesgo-algoritmico-y-la-proteccion-de-datos-personales/>

digitales²³⁰. Y, como he dicho, la protección de ambas identidades deberá diferir legislativamente.

El sesgo del alma y la caja de la privacidad: la solución real

Algunos creen que porque nuestros datos muestran nuestros deseos y nuestros miedos contienen el alma. Y, como ya he señalado, no es así. Simplemente contienen parámetros de conducta momentáneos y su evolución.

Todos los derechos contenidos en el genérico derecho a la privacidad contienen el derecho de exclusión. El derecho a la intimidad era el escudo del que se valían los seres humanos para defenderse de la curiosidad ajena²³¹. El de la propia imagen es la facultad de impedir la obtención, reproducción o publicación de su propia imagen por un tercero sin el consentimiento expreso del titular, sea cual sea la finalidad perseguida por quien la capta. El derecho al honor a que no se transgreda nuestra honra como derecho de la personalidad.

A su vez todos ellos tienen una faceta positiva de autodeterminación informativa: el consentimiento informado. Tanto desde la perspectiva del artículo 18.1 como del 18.4 CE se trata de la capacidad de control sobre dichos derechos individuales y el genérico a la privacidad. Así el TC centra cualquier lesión del derecho a la intimidad en la ausencia de un consentimiento válido para acceder a ese ámbito protegido por el derecho. En este contexto, dice el Tribunal Constitucional, “es innegable” que “algunos contornos de los derechos fundamentales al honor, a la intimidad y a la propia imagen pueden “quedar desdibujados” y que “la utilización masificada de estas tecnologías de

²³⁰ Daniel Solove. *The Digital Person: Technology and Privacy in the Information Age*

²³¹ Ignacio Villaverde Menéndez, *La intimidad, ese “terrible derecho” en la era de la confusa publicidad virtual*

la información añade nuevos problemas jurídicos a los ya tradicionales. Si bien es un hecho que el funcionamiento de las redes sociales permite la difusión de información personal, también lo es que puede significar una pérdida de control de la información suministrada por el propio usuario”. En ese sentido, el tribunal advierte “por obvio que resulte” de que “los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica”. El tribunal afirma que “el reconocimiento constitucional de los derechos fundamentales comprendidos en el artículo 18 de la Constitución conlleva la potestad de la persona de controlar los datos que circulan en la red social”.

En suma, existe un contenedor único llamado derecho a la privacidad que sustenta los derechos del artículo 18.1 CE. Todos esos derechos los tenemos en potencia con una expectativa general de que no se vulneren. Sin embargo, deberemos actualizarlos uno a uno con un consentimiento real e informativo (capacidad de autodeterminación). Para que nos entendamos entre los elementos que nos otorgó la Ilustración está la dignidad como seres humanos. La evolución ha configurado como elemento central de la dignidad el derecho a la privacidad. Si pudiésemos poner esos derechos etéreos dentro de una caja cerrada podríamos abrirla y cerrarla cada vez que nos interesase. Así quien quisiésemos nos vería, podría tomar una fotografía o criticar su contenido. Luego cerraríamos la tapa y volverían los secretos, la imagen o el honor a estar protegido. Esa caja cerrada llamada privacidad existe en el mundo analógico y es imposible que la reproduzcamos con exactitud, a diferencia del mundo digital donde sí. En el mundo digital se puede copiar. Todos vamos dejando pequeñas migajas digitales que unidas permiten conocer el contenido de la caja. Ahí radica el problema que nuestra privacidad se pierde entre los bordes de la caja. La sólida intimidad en el mundo digital se licúa como si pasase por un proceso de hidrólisis.

En el ciberespacio la información adquiere, como bien señala James H Moor²³² un “carácter grasiento” que dificulta su control. “En cuanto le damos al botón de enviar” sabemos que hemos perdido el control de la información y que la misma se ha tornado global²³³. El ciberespacio es eminentemente público donde la reproducción es ilimitada y encontrar un modelo de control es casi imposible. En el mundo analógico los tribunales y los servicios policiales suponen un elemento de control a todos aquellos que quieren ver nuestra caja: ya sean periodistas, policías, detectives, espías o, simplemente, cotillas. Como bien señala Moor, en la actualidad es un imperativo que creemos zonas de privacidad que permitan a los “ciudadanos planificar racionalmente sus vidas sin temor” a perderla. “Las zonas de privacidad contendrán situaciones privadas con diferentes tipos y niveles de acceso para diferentes personas. Es importante pensar en la privacidad en términos de “una cuenta de control / acceso restringido”, porque esta concepción fomenta el consentimiento informado tanto como sea posible y “fomenta el desarrollo de políticas prácticas, de grano fino y sensibles para proteger la privacidad”.

La paradoja de la privacidad

Tal y como hemos visto, la privacidad es uno de los problemas más importante de la era digital (por todos, Acquisti, Brandimarte y Loewenstein; Baruh, Secinti, y Cemalcilar; Trepte y Reinecke) junto con la seguridad. Las personas dejamos rastros digitales (paradoja de Pulgarcito) permitiendo que entidades privadas configuren nuestra personalidad digital. Sin embargo, algunos autores señalan que la preocupación por la privacidad (Antón, Earp y Young) y su desconfianza (Turow y Hennessy)

²³² Moor, J., Towards a Theory of Privacy in the Information Age. ACM SIGCAS Computers and Society, ACM SIGCAS Computers and Society 27(3):27-32

²³³ En el mismo sentido, Charles Ess en Digital Media Ethics.

no se ve reflejada en sus actividades lo que supone una “paradoja de la privacidad” (Norberg, Horne y Horne) ya que continúan compartiendo información en línea (Taddicken y Sanne Kruikeimeier, Sophie C. Boerman y Nadine Bol).

Sin embargo, estudios recientes de la Universidad de Tilburg²³⁴ demuestran que la paradoja de la privacidad es una reliquia del pasado. En una encuesta reciente señalan que las personas que no confían en la seguridad del medio tienden a realizar actividades de protección de su privacidad²³⁵. Un metaanálisis reciente encontró que las personas con mayores niveles de preocupación por la privacidad compartieron menos información en línea, era menos probable que usaran servicios en línea y más propensos a proteger su privacidad (Baruh). Las percepciones tienen un efecto positivo en las decisiones de compra en línea del consumidor. Metzger descubrió que la confianza es un antecedente clave para divulgar información personal información a un sitio web.

Sin embargo, continúa existiendo la verdadera paradoja del mundo: frente a lo gratuito nos vendemos. Así somos los humanos.

²³⁴ Sanne Kruikeimeier, Sophie C. Boerman & Nadine Bol (2020) Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy, *Media Psychology*

²³⁵ When we uncovered different subgroups of people's perceptions toward the social contract, we found that a moderately large group of people (20.62%) were labeled the highly-concerned users. These people do not trust online companies, have high levels of risk perceptions, and are concerned about their privacy. Hence, for these people the social contract is less reliable. Another interesting group is the people who are suspicious about the social contract; the wary users. This is also a relatively large group (27.99%) and consists of people who are similar to the highly-concerned user, but score less extreme on the three variables. It is difficult to compare these results with other typologies, especially as different methods are applied. However, when the highly-concerned and the wary user groups are combined, this finding is somewhat similar to (Sheehan, 2002). Sheehan (2002) found four types, and among these the alarmed internet users (3% in their study) and the wary internet users (43%). It could thus be argued that in society, almost half of the people perceive the social contract as less reliable and those people do not have the confidence that online businesses keep their data safe. This is also in line with others that found that the majority of European citizens perceive the privacy of personal information very important (Eurobarometer, 2016). Also many Americans distrust organizations (both public and private) in protecting their personal information when collected online (Rainie, 2016). Interestingly, only a very small proportion of people in society seem to perceive the social contract online as more reliable (4.75%). These carefree users have trust in online companies, experience little risk, and do not have much privacy concerns

Internet es aparentemente un cachorrillo de perro. Algo que nos facilita la vida. Como he dicho al principio Google es nuestro amigo. Y en el amigo se confía. No nos traiciona. Hablamos con los amigos, le contamos nuestros problemas y esperamos de ellos soluciones o, al menos, apoyo. Y mientras vamos cediendo información, privacidad. En Internet pasa algo similar. Cedemos información a cambio de que nos faciliten la vida. Luego llegan las quejas: la paradoja de la privacidad. Y debemos hacer algo para compaginar los intereses. Las empresas trabajan por nosotros y el coste son nuestros datos. Pero Google lo ha hecho tan bien que ya no podemos vivir sin sus plataformas. Es un bien público en manos privadas, una especie de autopista de pago. Y o pagamos o si queremos viajar gratis debemos dar algo a cambio: nuestros datos. Por eso es necesario cambiar el contrato social para que se adapte a nuestra personalidad digital.

La exigencia de transparencia

“La privacidad no ha muerto, pero está en peligro y estamos en un momento crítico para salvarla”, dice el protagonista de la serie de Netflix El Gran Hackeo, David Carroll, un profesor universitario radicado en Nueva York, que se convirtió en noticia por su disputa con Cambridge Analytica a la vez que intentaba recuperar sus datos en manos de Cambridge Analytica señala que “lo peor ha llegado”. Explica que analiza cada una de las aplicaciones que instala en los teléfonos de sus hijos para saber qué datos recopilan.

Pero su proceso judicial contra Cambridge Analytica es, precisamente, lo que nos interesa ahora. Cuando David Carroll solicitó a Cambridge Analytica (CA) su perfil de votante, se asombró de que la respuesta llegara firmada por Julian Wheatland, director operativo de Strategic Communication Laboratories (SCL). Carroll demandaba conocer todos los datos per-

sonales que tenía CA y las fuentes de donde los obtuvo. Carroll dijo que inició la demanda como parte de «un deseo general de asegurarme de que mis datos personales no se usen para propósitos que considero perturbadores o ilegales», algo que le resulta «particularmente verdadero en lo que respecta a mis opiniones políticas», señala The Guardian. Pero si en algo tiene importancia el documental es que no se centra tanto en el usuario en sí, sino en quienes proveen, administran, mantienen las redes sociales, y en terceros que se benefician de la información que de ellas obtienen. Y ahí está el elemento principal de todo esto. Los usuarios no nos podemos mantener ajenos culpando a terceros. Queremos información, damos información y no exigimos transparencia.

Dependemos de las plataformas tecnológicas y es a ellas a las que debemos exigir transparencia. Según el portal de ciencia de nuestro Gobierno “las Plataformas Tecnológicas son estructuras público-privadas de trabajo en equipo lideradas por la industria, en las que todos los agentes sistema español de Ciencia-Tecnología-Innovación interesados en un campo tecnológico trabajan conjunta y coordinadamente para identificar y priorizar las necesidades tecnológicas, de investigación y de innovación a medio o largo plazo”. Ellas son las que deberán asegurar que exista transparencia en las plataformas empresariales para que los ciudadanos concedamos nuestro consentimiento.

Algunos exigen la recuperación de los datos. La realidad es que debemos exigir el control absoluto de nuestros datos. Tenerlos controlados en nuestra plataforma personal y asegurados por las plataformas tecnológicas públicas. Esa es nuestra caja personal. En caso contrario mediante las técnicas de manipulación que hemos explicado se puede conseguir que vean el mundo como una parte del *stablishment* quiere. ¿Cómo? Mediante *fake news* o exageraciones que permitan hacer creer que lo que nos

interesa. Pero eso no es llegar al alma de la persona. Porque los datos no tienen alma, a pesar de que los activistas de la *hyper-privacy* nos bombardeen con sus ideas. Los sesgos están ahí y el Sistema permite que nos moldeen a su interés. Esa fue la estrategia de Cambridge Analítica: analizan tus deseos y dirigen el mensaje para moldear tu comportamiento. En ese sentido, votar a Trump o votar el Brexit.



❖ CAPÍTULO 10. HABLEMOS DE DINERO: UNA RENTA BÁSICA POR NACER

Los datos son dinero, son el pan con el que nacemos bajo el brazo. ¿A cambio de qué?: de nuestros datos. Los famosos, por ejemplo, modulan su intimidad según comercian con sus derechos de la personalidad. Sé que la democracia liberal no tiene raíces emocionales nuestro país, pero en España ya se vende la privacidad. En nuestro país existe el derecho de los famosos, modulado por el interés público que no por el interés del público (cotilleo). Así señala la STC 19/2014: “Procede declarar que si bien es aceptable que el concepto de interés noticiable sea aplicado a los programas de entretenimiento, dicho carácter del medio o de las imágenes publicadas no permite eludir ni rebajar la exigencia constitucional de relevancia pública de la información que se pretende divulgar al amparo de la libertad de información. De aceptarse ese razonamiento, la notoriedad pública de determinadas personas –que no siempre es buscada o deseada– otorgaría a los medios de comunicación un poder ilimitado sobre cualquier aspecto de su vida privada, reduciéndolas a la condición de meros objetos de la industria de entretenimiento”.

Y nuestros tribunales siguen en este sentido la sentencia del Tribunal Europeo de Derechos Humanos de 24 de junio de 2004, caso Von Hannover v. Alemania, el asunto Carolina de Mónaco que pone el acento en la contribución de la publicación de fotografías o artículos en la prensa al debate de interés general, “sin que la satisfacción de la curiosidad de una parte del público en relación con detalles de la vida privada de una persona pueda considerarse contribución a tal efecto pese a la notoriedad de esa

persona”²³⁶. En nuestro país, el ejemplo paradigmático es la STS 702/2016 sobre Rocío Carrasco donde se señala que: “Las referidas intromisiones no pueden considerarse amparadas por la libertad de expresión, ni por la libertad de información como más especialmente considera la sentencia recurrida, porque si bien esta sala ha reconocido que en los actuales programas de televisión de crónica social o entretenimiento puede haber un tono de cierta agresividad en cuanto socialmente tolerado (sentencias 92/2015, de 16 de febrero, y 497/2015, de 15 de septiembre), y si bien es cierto que la demandante gozaba de cierta celebridad por ser hija de una cantante y un boxeador y haber aparecido en los medios, y que el demandante participaba de tal celebridad por ser pareja de la demandante, no lo es menos que siempre han demostrado querer preservar su intimidad personal y familiar y proteger su honor, como se desprende de las ya citadas sentencias 169/2011 y 808/2013, y, además, de las sentencias 1129/2008, de 20 de noviembre, 660/2010, de 3 de noviembre, 603/2011, de 20 de julio, y 96/2012, de 20 de febrero, a las que incluso cabe unir la sentencia 810/2013, de 27 de febrero”.

Pues bien, en nuestro país (y muchos otros) ser hijo de un famoso supone un sueldo nada más nacer a cambio de sus fotografías (derecho a la propia imagen) o sus declaraciones (derecho a la propia voz). Los medios de comunicación pagan por conocer su vida y los famosos modulan cuándo quieren ceder parte de sus derechos a la privacidad a cambio de salario.

Derecho sobre los datos

Por eso, el sistema que propongo es similar, pero para todos los ciudadanos. Ceder nuestros datos a las empresas entrarían den-

236 Fayos Gardo, A. (2000). *Derecho a la intimidad y medios de comunicación*. Madrid: Centro de Estudios Constitucionales

tro del patrón de modulación. El usuario determinaría cuándo y cómo cede los derechos, a cambio de cuánto y cuándo acaba la relación. Las personas con nuestro contrato social tendremos un alter ego, persona digital, que tendrá un sueldo nada más nacer. Sólo por existir valdrá dinero lo que valgan sus datos, con la advertencia clara de que cuando ceda todos sus datos y se quede sin ellos, se convertirá en un homeless.

“Cada dato que compartes en Facebook es tuyo”, fue una de las declaraciones de Mark Zuckerberg, fundador de Facebook, cuando fue interrogado por el Senado sobre sus relaciones con Cambridge Analítica. “Zuckerberg solo quería decir que los usuarios deberían controlar quién ve sus publicaciones. Pero tal vez deberíamos tomarlo literalmente. ¿Qué pasa si los datos personales tienen un valor como cualquier otra propiedad? ¿No deberían los propietarios de los datos ser compensados por su uso”, se preguntan Jennifer Granholm, ex gobernadora de Michigan y asesora principal de Media Matters, y Chris Eldred, asesor de políticas y comunicaciones del American Jobs Project, en una columna publicada por la CNN²³⁷.

El Finantial Times señaló que “los datos habían superado al petróleo como el activo más valioso del mundo. Empresas como Facebook, Google y Amazon han creado monopolios ricos en datos que explotan sin remordimientos los activos y comportamientos digitales de sus usuarios: nosotros”. Facebook es ahora el mayor broker de datos del mundo. Su modelo de negocio se basa únicamente en extraer valor de nuestros activos digitales personales.

Por eso los usuarios deben saber que sus datos son privativos de su personalidad digital, igual que sus casas lo son para su perso-

²³⁷ <https://www.infobae.com/america/tecno/2018/04/16/deberia-facebook-pagar-a-los-usuarios-por-acceder-a-sus-datos/>

nalidad analógica. Si Google o Facebook desean usar sus datos, deben buscar el consentimiento completo e informado, explicar todas las formas en que se utilizará la información, darle la posibilidad de no participar y en caso de querer compensarlo económicamente. Airbnb ha permitido a las personas de todo el mundo poner sus hogares a la venta y los usuarios piden permiso para ser huéspedes, llegan a un acuerdo y pagan un precio a cambio de las llaves. Ahí está la clave de todo. Airbnb cobra una comisión por la gestión y por el uso de los datos de los huéspedes: saben qué perfil económico viaja a determinadas partes, en qué fecha, qué buscan y qué desean. Cuando acaba el contrato saben si son limpios, si les gusta la fiesta, si han viajado en familia o con amigos y demás. En el caso de Facebook, que ofrece su servicio de forma gratuita, la publicidad es su principal forma de ingresos. El año pasado, la red social tuvo ingresos por valor de 40,7 mil millones de dólares a nivel mundial. Cerca de USD 19,5 mil millones fueron de publicidad en los Estados Unidos y Canadá, donde cuenta con 235 millones de usuarios activos por mes. Cobrar por nuestros datos no es descabellado.

Una encuesta realizada en 2017 por la empresa de estudios de mercado alemana GfK señaló que la gente está dispuesta a intercambiar su información privada por descuentos o regalos. Así, el 38% de los ciudadanos chinos, el 30% de los mexicanos y el 29% de los rusos afirman que sí cederían sus datos online por una recompensa. En España esta cifra se reduce al 16%. Solo falta que exista un acuerdo global. Pero ya existen empresas que negocian con datos de forma transparente. DataWallet permite a los usuarios crear un perfil online para que lo puedan compartir con organizaciones interesadas y así obtener ingresos. Según esta app, los usuarios pueden ganar entre USD 1 y USD 50 por la venta de sus datos personales. Existe una calculadora online, llamada Totally Money, donde se puede realizar un simulacro para ver cuánto está dispuesto el mercado a pagar ciertos datos.

Renta básica

Si las transformaciones son reales, ¿por qué tardan tanto en llegar a nuestros bolsillos en forma de dinero? Entiendo que el concepto de renta básica es contrario al libre mercado como señaló Juan Ramón Rallo, profesor de Economía en la Universidad Francisco Marroquín²³⁸ “Estoy moralmente en contra de la renta básica porque es un atentado contra la libertad del individuo”. Sin embargo, Juan Torres López, catedrático de Economía Aplicada de la Universidad de Sevilla, en su libro *Renta Básica* plantea, entre otros aspectos, el de “la renta básica como subproducto del ataque neoliberal al Estado del bienestar” y descubre que “con una minúscula tasa del 0,1 por ciento sobre el volumen total de las transacciones [que se realizan en el mundo] se podría financiar sobradamente una renta básica universal en todos los países del planeta sin que ningún Estado tuviera que establecer ningún tipo de impuesto adicional”. Es verdad, señala Marta Ávila en *Infolibre*, que “se trata de cálculos brutos, de trazo grueso y una tasa así necesitaría un gran acuerdo internacional, una tecnología apropiada, mecanismos adecuados de liquidación y luego de reparto (porque no tendría sentido que la renta básica fuese igual en todos los países o incluso territorios ...). Pero todos esos no son sino problemas técnicos que se pueden resolver con más o menos dificultad con los medios con los que hoy día disponemos. Lo importante es que no se puede afirmar que la financiación de una renta básica universal, ni siquiera a escala planetaria, sea imposible porque no hay recursos”²³⁹. Pues bien, la solución a ese problema es un acuerdo global sobre los datos de carácter personal.

²³⁸ https://www.infolibre.es/noticias/opinion/plaza_publica/2019/03/31/pacto_social_constitucion_democracia_game_over_93342_2003.html

²³⁹ *Infolibre*, op. cit.

El premio Nobel de Economía Joseph Stiglitz aboga por buenos sistemas de protección social pero no por proteccionismo y, en este sentido, no cree que la renta básica universal sea la solución, porque, asegura, “yo no creo que nadie quiera recibir solo un cheque con dinero sin hacer nada”²⁴⁰. En su último libro señala que la regulación del mercado de los monopolios tecnológicos podría adoptar varias formas, desde la transparencia (control entre los que se publica y la seguridad de la protección de los datos) hasta las prohibiciones. Sin embargo, aboga por la asignación de un precio mínimo establecido por el Gobierno cuando una empresa use los datos personales. Incluso señala que se podría fijar un impuesto al uso o al almacenamiento o tratar los datos como un bien público. Sin embargo, tal y como ya se ha dicho, los datos anonimizados que sirvan para la mejora del bien común son los bienes públicos. En cuanto individualizan a una persona pasan a ser un bien privado.

Y, por tanto, la renta básica por nacer no se aplicaría a los Estados. Sería una renta básica establecida con la llegada al nuevo contrato social capitalista de las redes de la tecnología. Las empresas de pañales, las de mobiliario infantil, las de ropa para bebé pondrían a disposición del nuevo nacido de un paquete de dinero a cambio de sus datos y de que, a su vez, esas empresas cobren a las madres y los padres del nuevo nacido por los productos que venden.

El doble contrato social

En el momento en que no tener redes sociales genera al ciudadano una visión de ser antisocial es fundamental regular y proteger los sistemas de comunicación informática. Por tanto, la tensión está en si se puede o no garantizar la protección. Estas

²⁴⁰ <https://www.publico.es/economia/jospeh-stiglitz-pasaran-anos-espana-vuelva-normalidad.html>

aproximaciones recogen los postulados de Mason para quien la armonización de derechos en el mundo digital se daría gracias a la formulación de un nuevo «contrato social»²⁴¹.

Nissenbaum sienta en 1997 “las bases para abordar la salvaguarda efectiva de las informaciones privadas en entornos digitales y lo hace al enunciar su teoría Privacy as contextual integrity. La idea primigenia, no obstante, fue posteriormente reformulada por la autora bajo la influencia de académicos como Solove, Benkler o Kerr y teniendo en consideración muchos de los posteriores desarrollos de las Tecnologías de la Información y Comunicación”²⁴². En este sentido, la teoría de la contextual integridad “está diseñada para considerar cómo la introducción de una nueva tecnología en un determinado contexto cambia las normas que gobiernan el flujo de información, lo que significa que es capaz establecer qué datos son o no pertinentes en cada contexto, aunque se trate de un escenario digital. Afirma la autora al respecto: Si la introducción de una nueva tecnología o práctica en un determinado contexto se encuentra en conflicto con las normas de flujo de información establecidas, una bandera roja es desplegada, indicando que la integridad contextual ha sido violada. Parte de la doctrina acierta al señalar que el bien jurídico protegido en el acceso informático es la seguridad de las comunicaciones”²⁴³.

En suma, en la protección de la intimidad y vida privada, debemos capacitar al individuo para ejecutar su propia autodeterminación informativa. Un ciudadano informado en una relación transparente con las empresas o entidades públicas que gestionen sus datos es capaz de llevar a cabo, de manera activa,

²⁴¹ Mason, R. O. (1986): «Four ethical issues of the information age», en *MIS Quarterly*

²⁴² Citado en *La protección de la intimidad y vida privada en internet*, op cit.

²⁴³ Amaya Noain Sánchez. Op cit.

su potestad sobre sus informaciones privadas y personales “valorando, en consecuencia, cuándo desplegar cierta información sin que eso suponga un riesgo para la preservación de su ámbito reservado”²⁴⁴.

Si creemos en el ciudadano digital como la persona con derechos y deberes debemos llegar a la conclusión que la persona analógica tendrá una nacionalidad y un contrato social vinculado al Estado y la digital una supranacionalidad por cuanto se relaciona sin fronteras. Por tanto, en el análisis que se está realizando la personalidad digital deberá ser supranacional. Debemos crear una especie de ONU donde se nos proteja y donde se establezcan las mismas reglas del juego en el mundo digital. La entidad protegerá las redes de comunicación, legislará y juzgará. Estamos hablando de un futuro donde el mundo digital será una suerte de Estado Federal Mundial. Y cada uno de los países seguirán manteniendo su nacionalidad en su forma analógica.

Pero igual que en el contrato social inicial cedimos parte de nuestra libertad a cambio de seguridad, en la actualidad existirán dos contratos sociales. El primero, analógico e inmutable y el segundo, digital, donde cederemos al Estado parte de nuestra privacidad (el acceso a nuestro banco privado de datos) a cambio de que proteja nuestra morada informática y los sistemas de comunicación. Mark Zukerberg habla de regulación al Financial Times, el presidente de Microsoft también cree que es necesaria. Hay, por tanto, una creciente sensación de que el poder del mercado de los datos debe ser frenado. Es radicalmente necesario determinar quién es el propietario de los datos. Stiglitz lo deja claro. La propiedad de los datos es de uno mismo. Eso implica que cualquier “empresa que desee usarlos podría obte-

²⁴⁴ Amaya Noain Sánchez. Op cit.

nerles a un determinado precio, y el individuo podría proscribir que los explotaran de cualquier forma”²⁴⁵. Ahí tenemos la renta básica.

Sistema de gestión de tráfico de datos

El sistema de propongo es similar a la red de Baran. Un sistema centralizado de control y seguridad con sistemas dispersos de intercambio de información. “La gestión del tráfico ofrece dos clases de poder. El primero, el poder de leer la información de las cabeceras de los paquetes, para comprobar que cumplen los requisitos del protocolo. Segundo, el de regular su itinerario. La suma de toda esa información se llama metadatos y tienen un enorme valor. Para que una red siga siendo descentralizada es crucial que los metadatos se dispersen”²⁴⁶.

El 85% de la información que producimos no se utilizan. En una carta abierta, Úrsula Von Der Leyen, Presidenta de la Comisión Europea, señala que una de las principales estrategias de la UE es la transformación digital como impulsora de la nueva economía ante el desafío mundial de la digitalización de esos datos no utilizados a los que me refería. “Pero la transformación digital, no puede dejarse al azar”, señala y se debe garantizar que los “derechos a la privacidad” sean “los mismos en línea que fuera de ella”.

Parte, por tanto, la Comisión Europea de un error de base. Los derechos a la privacidad son diferentes, como se ha dicho, en la era pre digital y post digital. Señala que, además, si queremos que Europa sea líder se debe potenciar el acceso y la recopilación de los datos: “la mina de oro por descubrir y utilizar” en la econo-

²⁴⁵ Stiglitz, op. cit.

²⁴⁶ Marta Peirano, op. cit.

mía de datos de futuro. Señala que se debe potenciar la recogida y explotación de datos no personales (señala por ejemplo los datos meteorológicos) para que sirvan de base “a nuevos productos o servicios más eficientes y sostenibles”. Señala que la UE “elaboraremos un marco legislativo y normas de funcionamiento para los espacios de datos europeos que permitirán a empresas, gobiernos e investigadores almacenar sus datos y acceder a los compartidos por otros”. Este conjunto de datos, remarca, impulsarán, a su vez, “la confianza en la inteligencia artificial de Europa”.

Todo ello en pos de una “soberanía tecnológica”, que para la Presidenta de la Comisión se resume en “la capacidad que debe tener Europa para tomar sus propias decisiones, basadas en sus propios valores y respetando sus propias normas”. Sin embargo, señala que el punto de partida debe ser la “protección personal” y añade que “Europa tiene ya las normas más estrictas del mundo y ahora daremos a los europeos las herramientas que necesitan para asegurarse de que su seguridad es aún mayor”.

Las crisis de Facebook y Cambridge Analítica o libros como *Despertar del sueño tecnológico*, Ekaitz Cancela señala que hay que quitarle a Google y Facebook la propiedad de las infraestructuras digitales. “Ellos no proveen servicios públicos: nos proveen de servicios premium” ha puesto sobre la mesa la necesidad de devolver el control de la identidad a los usuarios. Digitalización significa infraestructura. La lógica empresarial tiende hacia la centralización del poder. Los legisladores de la UE han alcanzado hoy un acuerdo para plataformas digitales online dirigido a reducir el poder que estas grandes empresas tienen en la actualidad. Sin embargo, a pesar de las críticas, “inversores, consumidores y reguladores parecen no haber cambiado su comportamiento”, señala el *New York Times*²⁴⁷ que

²⁴⁷ <https://www.nytimes.com/es/2017/10/16/espanol/los-peligros-de-los-gigantes-tecnologicos.html>

añade: “La gente aún espera con ansias el nuevo iPhone. Facebook tiene más de dos mil millones de usuarios. Al presidente Donald Trump le gusta criticar a Amazon en Twitter, pero su administración ignoró las peticiones de una revisión rigurosa de la compra de Whole Foods por parte de Amazon”. Europa, sin embargo, apuesta por un sistema que reconoce al usuario el derecho a controlar sus datos personales y gestionar su capacidad para llevarse los datos de una plataforma a otra.

La descentralización de los datos hará que tengamos el poder de nuestros propios datos y que podamos tener nuestra propia “caja fuerte de datos” desde el nacimiento de nuestra personalidad en el mundo digital. Esa caja nos permitirá determinar a quién ceder los datos y a cambio de qué. Al Estado (Hacienda) le cederemos el acceso a nuestros ingresos y nuestros pagos para que de forma automática nos diga cuántos impuestos pagar. A cambio nos dará seguridad, infraestructuras y bienestar. A las empresas que nos faciliten nuestra vida digital le abriremos parte de ese consentimiento a cambio de dinero o servicios.



❖ CONCLUSIONES

- La personalidad se ha dicotomizado en dos. Por un lado, tenemos la personalidad analógica marcada territorialmente por las obligaciones que nos imponen nuestros Estados.
- Por otro lado, tenemos una personalidad digital nada más nacer que es universal y que requiere de un contrato social único, basado en la confianza en el sistema.
- El nuevo contrato social que rijan nuestra identidad digital deberá exigir la descentralización de los datos y la devolución de los mismos desde las grandes corporaciones a los ciudadanos.
- El sistema requiere de una red donde el nodo central conecta a todos los demás miembros de la red. Este nodo central debe estar gestionado por un organismo multilateral (similar al de la ONU) que lo proteja.
- Los ciudadanos, además, tendremos como derecho primordial el uso de las redes sin ceder nuestros datos.
- Los datos que generemos nada más nacer se acumularán en una caja fuerte digital especial que estará en el interior de nuestros ordenadores o de nuestros smartphones.
- Esa caja fuerte deberá estar protegida por nosotros y por el organismo multilateral que proteja el nodo central. La integridad y la seguridad de los datos es más importante que la privacidad, como lo fue la integridad personal en el primer contrato social.
- Para usar los servicios de comunicación (redes, Google, app etc) no le cederemos nuestros datos y mucho menos de forma gratuita. Las empresas de telecomunicaciones pondrán precio a sus servicios y los pagaremos con dinero o con nuestros pocos datos mediante cesiones personales que no permanentes.
- Los datos de carácter personal estarán siempre almacenados en nuestra caja digital y solo saldrán temporalmente mediante el

consentimiento expreso, cuando queramos usar un bien o servicio o de forma tácita para cumplir con el contrato social territorial.

- El Estado con el que mantenemos el contrato social analógico hará lo propio: consultará nuestros datos de compras, de ingresos y gastos en nuestra caja digital y nos ofrecerá un modelo provisional de declaración de la renta. En caso de que le deneguemos el acceso o comentamos un delito serán los tribunales los que solicitarán al organismo multilateral centralizado para que le de acceso forzoso.
- Con este sistema los ciudadanos tendremos un sueldo mínimo nada más entrar nuestros datos en la caja fuerte personal donde se almacene nuestra huella dactilar, los datos médicos y demás necesidades del recién nacido. Con esos datos negociaremos ventajas con empresas de productos infantiles que pagarán por los mismos o negociarán descuentos a cambio de datos.



Discurso de contestación

Excmo. Sr. Dr. Fermín Morales Prats

Excmo.Sr.Presidente
Excmo.Sres.Académicos
Excmos. e Ilmas. Autoridades
Sras. y Sres.

❖ I. INTROITO Y LAUDATIO

Después de haber escuchado con atención y leído pormenorizadamente el discurso de ingreso en esta Real Corporación del Académico de Número Excmo. Sr. Dr.D. Francisco Marco Fernández me corresponde el privilegio y el compromiso de contestar un profundo y filosófico discurso como es el que ha pronunciado el recipiendario.

La Real Academia Europea de Doctores, a través de su Presidente, el Excmo.Sr.Dr.D.Alfredo Rocafort Nicolau, me atribuye la responsabilidad de este discurso de contestación. Dejo constancia aquí de mi agradecimiento por la confianza depositada para afrontar el encargo, de modo que declaro públicamente la aceptación del honor que se me hace, confiando en que sabré estar a la altura que exige el presente acto. Siempre es estimulante procurar dar cumplida respuesta a planteamientos novedosos, a veces provocativos intelectualmente, que se desprenden del discurso de ingreso del Académico Dr. Francisco Marco.

El discurso al que debo dar contestación aporta una reflexión actual sobre problemas políticos, sociales y jurídicos candentes.

La vertiginosidad cotidiana muchas veces no nos da respiro para atender a reflexiones profundas como las pronunciadas por el recipiendario en su discurso. Además, el discurso de ingreso viene trufado de planteamientos esperanzadores, casi diría que utópicos, lo que no es frecuente en nuestros días. Por tanto, el discurso supone una apuesta por superar las distopías que inundan actualmente los planteamientos intelectuales.

El discurso del Dr. Francisco Marco debe ser analizado en profundidad porque permite extraer un diagnóstico del momento en que se encuentra nuestra sociedad y principalmente de cómo hemos metabolizado grandes cambios tecnológicos en nuestra vida cotidiana sin reparar en las consecuencias que comporta. Por consiguiente, el Dr. Marco nos reta a efectuar una reflexión de hacia dónde nos dirigimos y sobre todo si queremos afrontar el futuro con nuevas reglas de equilibrio entre preservación de los derechos del ciudadano y desarrollo tecnológico irrefrenable.

En el planteamiento del recipiendario evidentemente hay reflexiones jurídicas, propuestas de equilibrio en lo que vendría a ser un nuevo contrato social en un contexto de nueva revolución tecnológica. Pero, más allá de lo jurídico, el discurso aporta reflexiones políticas sociológicas y filosóficas, suscitando así un diagnóstico de futuro cultural en el que el ciudadano pueda redefinir el estatuto de sus derechos fundamentales. Ciertamente quien les habla no profesa una visión del futuro inmediato tan optimista, porque como vengo teorizando desde hace años, estamos sumidos en una suerte de nueva Edad Media, contexto en el que reina la incertidumbre, la inseguridad y la pérdida de garantías para el ciudadano. El discurso del Dr. Marco reclama que se encienda la luz, por cuanto divisa un horizonte de futuro en el que fuera posible atisbar una suerte de nuevo renacimiento con preservación de los derechos del ciudadano.

Las palabras del Académico Dr. Francisco Marco suponen la confirmación de una sólida carrera intelectual, el discurso nos muestra su capacidad analítica profunda, intentando esclarecer cuestiones fundamentales en un contexto en el que impera el desconcierto y la ausencia de modelos de sociedad óptimos que permitan sustentar ideologías que diseñen criterios colectivos de felicidad.

Permítaseme, Sr. Presidente, que eche la mirada hacia atrás para retroceder en el tiempo al objeto de trazar un brave semblanza del currículum del recipiendario. Seguramente me cabe el singular honor de ser testigo privilegiado del recorrido personal y profesional del Dr. Francisco Marco, Académico de Número de nuestra Real Corporación.

Conocí al Dr. Francisco Marco en otoño de 1995, venía con la que luego sería discípula en mi universidad Esther Morón. Me los presentó mi colega, y a pesar de ello amigo, Cristóbal Martell, quien los avalaba por cuanto había sido su profesor de Derecho Penal durante la licenciatura que el recipiendario y Esther Morón habían cursado con éxito en la Universidad Abad Oliba- CEU.

Francisco Marco quería hacer la tesis doctoral sobre aspectos relacionados con la “privacy” y con la investigación privada, dado que en 1994 ya había obtenido el grado de investigación privada en la Universidad de Barcelona. Por aquel entonces el recipiendario ya trabajaba también con su madre, Marita, que regentaba una reputada agencia de investigación privada. Demasiados proyectos a la vez pensé, y ubiqué al Dr. Marco en el grupo de doctorandos que no finalizarían la tesis, por cuanto la condición humana expresa, en muchos casos, grandes ilusiones iniciales para obtener el doctorado y gran cansancio a la hora de ejecutar el trabajo. Por supuesto desconocía en aquel entonces

la capacidad de trabajo y tenacidad que atesora el Dr. Marco. No obstante, me llamó la atención la ilusión con la que se integró en las vivencias y quehaceres del grupo de profesores de mi escuela universitaria, comandada por el Dr. Gonzalo Quintero.

Finalmente, la tesis fue leída, bajo mi dirección, en la Universitat Autònoma de Barcelona en el año 2002, bajo el título “La investigación privada y el derecho a la privacy”, obteniendo la calificación de sobresaliente “cum laude”.

Con anterioridad a la obtención del título de doctor, Francisco Marco ya había sido precursor de trabajos sobre la problemática que suscitaba Internet frente al derecho a la “privacy”. En esta órbita de inquietudes se sitúa su trabajo doctrinal publicado bajo el título “La protección de datos personales automatizados en las redes mundiales de información” en 1998. La segunda mitad de los años noventa fue de gran actividad formativa del recipiendario; en 1996 cursó el Máster de Derecho de sociedades del Il·tre. Colegio de Abogados de Barcelona.

En ese periodo Francisco Marco también se adentró en cuestiones procesales. En 1999 publicó junto con quien esto suscribe, el estudio doctrinal “La naturaleza jurídico-procesal del detective privado: el testigo-perito”; posteriormente el hoy recipiendario sería uno de los impulsores de la introducción de la figura del investigador en la Ley de Enjuiciamiento Civil. También en los años 1998-1999 el Dr. Marco me embarcó en un ambicioso proyecto de recopilación legislativa, concordada y comentada, el “Código de seguridad privada”, publicado por la editorial Aranzadi.

En el año 2000 obtuvo el Premio nacional de Doctrina, convocado por la editorial DATADIAR, por el artículo “La monitorización del correo electrónico en la empresa”.

Después de la obtención del doctorado se suceden las publicaciones siempre en la encrucijada entre garantías jurídicas y procesales e investigación privada. En 2003 y 2004 publica sucesivos artículos en la Revista *Economist & Jurist*: “Los desechos de basura como medio de prueba”, “Los detectives y la ley del Jurado” y “Los seguimientos realizados por detectives privados”.

El beneficiario desde hace 25 años dirige uno de los mayores grupos de inteligencia empresarial en España y es el representante mundial para España de la *World Association of Detectives* y fue uno de los introductores de la *Council of International Investigations*.

Ha escrito una docena de libros de divulgación de aspectos jurídicos y de investigación privada: (“Objetivo Intervida” 2007, “El control en la empresa: cómo investigar legalmente la competencia y a los empleados” 2008, “Detectives SA: el negocio del investigación preventiva en las empresas” 2009, “El método” 2013, “la preparadora de juicios” 2015, “Real politik” 2015, “Cazando infieles” 2016, “Los secretos del Alba” 2017, “Operación Cataluña: la verdad oculta” 2017, “De la operación Cataluña al 155: la historia completa de cómo se llegó a la intervención del Gobierno de Cataluña” 2017, y “La España inventada” 2020.

Terminaré esta pequeña “laudatio” introductoria tomando prestadas frases de Salvador Sostres, publicadas en ABC (7/11/2019 “Solíamos ganar”), sobre el hoy beneficiario:

“... Siempre he pensado que, aunque lo de investigador privado me parece una labor absolutamente respetable, y necesaria, no hace justicia a lo que Paco realmente hace, y en este mundo tan extraño, y tan ingrato que nos ha tocado vivir, la mayor parte de problemas que tenemos se basan en que estamos des-

orientados. Esa labor de diagnóstico, esta clarividencia que Francisco Marco posee, y su quirúrgica capacidad para saber quién está en disposición de poder ayudarte mejor, es muchas veces más importante que cualquier otra indagación. Aunque me temo que no seré original en mi comparación, Paco me recuerda a “La soledad era esto” de Juanjo Millás, y a su protagonista que acude a un investigador privado para que le escriba informes sobre su propia vida. Cuando Paco te escucha, te entiende, y te ayuda a conseguir lo que quieres, tienes la sensación de que ha buscado en medio mundo para ayudarte, y en realidad apenas ha salido de ti...”



❖ II. CONTESTACION AL DISCURSO DE INGRESO

Tras el magnífico e intenso discurso de ingreso, que ha leído el Académico recipiendario, Dr. Francisco Marco, en el que no aborda con aguda visión constructiva nada más y nada menos que cuestiones esenciales del futuro social de la humanidad, sería cuanto menos una frivolidad por mi parte inmiscuirme con profundidad en tal argumentación. Efectuaré, sin embargo, algunas valoraciones y puntualizaciones porque el discurso de ingreso es merecedor de ello.

Arranca el recipiendario su discurso advirtiéndonos de las consecuencias de lo que denomina “el totalitarismo de la atención”, para significarnos que cada vez somos más digitales en la medida que hemos menguado en nuestra vida analógica, contexto éste último en el que impera el individualismo y el aislamiento. Esto se traduce en una suerte de contrasentido: imperio de la “privacy” en el mundo analógico frente a una creciente transparencia (visibilidad) en Internet. De ahí el título que preside el discurso de ingreso “Disociados (desdoblados)”. El Dr. Marco pretende afrontar esta dicotomía de personalidad jurídica (social y psicológica), que de manera progresiva nos arrastra a la pérdida de la identidad digital, preso el individuo de la continua cesión de datos para ser visible en el mundo digital, en suma, para existir en esa dimensión. ¿Cómo hacer frente a esta suerte de dictadura? El individuo compulsivamente ejerce la transparencia ante el buscador, la captura de datos es imparable, captura que a su vez produce nuevos contenidos nuevos perfiles de usuario, que permiten suscitar nuevas necesidades al navegante virtual, La cadena es interminable e imparable.

El contexto descrito es preocupante, pérdida de libertad en la medida que somos desposeídos de nuestra personalidad digital o, peor aún manipulados en cuanto a su desenvolvimiento. Francisco Marco, con sagacidad, no se conforma con el lamento, con la descripción lúcida del problema. Esboza una solución de equilibrio para preservar los derechos del ciudadano; propone nada más ni nada menos que un nuevo contrato social: navegar y ceder datos sí, pero de manera garantizada y con contraprestaciones.

¿Es pertinente esta propuesta? Estimo que sí. Debemos superar la cultura del lamento. Cesar en las redefiniciones jurídicas del derecho a la privacidad, que en su “nouvelle vague” se ha convertido en la aspiración de navegación en las redes con expectativas de anonimato. Debo reconocer que, en la actualidad, el discurso garantista tradicional o se redefine o morirá de impotencia.

Se ha generado la cultura de la transparencia. Participar en las redes es ser transparente; quien no participa es opaco y, por tanto, lejano a la verdad. Verdad y transparencia son mantras de la “nueva edad media tecnológica”. El filósofo Byung-Chul HAN, en su obra “La sociedad de la transparencia” desvela la falacia del planteamiento; el discurso público de la transparencia en realidad enmascara la apuesta por la vigilancia y el control del ciudadano, en la sociedad ha desaparecido la confianza; como dice HAN “se trata de una coacción sistémica”, de la que dimanan imperativos de conducta, principalmente económicos, absorbidos acriticamente por el ciudadano; las cosas se hacen transparentes en la medida que se despojan de su singularidad; en suma, la sociedad de la transparencia es “el infierno de lo igual”. El igualitarismo expresa así la medida de lo justo, de lo correcto.

Y este “totalitarismo de la atención” que describe con lucidez Francisco Marco, no es neutro, produce devastadores efectos. Volvamos de nuevo a HAN, ahora situados en su obra “La so-

ciudad del cansancio” (*Müdigkeitsgesellschaft*): la sociedad actual se caracteriza por expresar un paisaje social patológico de trastornos neuronales; el exceso de positividad produce depresión, trastorno por déficit de atención o por hiperactividad, trastorno límite de la personalidad y agotamiento.

La segunda falacia gira en torno a la cultura de la verdad; somos transparentes y, en consecuencia, veraces. La personalidad digital nos sitúa en un mundo en el que la verdad comunicativa quiere ser moneda de cambio. Aquí la refutación si cabe debe ser más radical. Debemos refutar la famosa frase de NIETZSCHE:” todas las verdades que se callan son venenosas”. La pretensión de vertebrar un sistema social sobre exigencias radicales de verdad es peligrosa. Produce efectos devastadores, incluso inquisitivos. Las pretensiones de verdad a cualquier precio expresan una cultura inquisitiva. El espacio en el que la verdad se calla, se oculta, no necesariamente debe ser ocupado por la mentira. Nuestra vida, nuestra cultura está presidida por los claroscuros, por los tonos grises. La condición humana no puede ser acreedora a la verdad absoluta, si se me permite cierto grado de cinismo es básico para la convivencia, incluso para la preservación de la identidad. ¿Sería posible la paz social si supiéramos permanente todo lo que piensan y hacen lo demás? Evidentemente no. De ahí el acierto de Francisco Marco cuando identifica los riesgos de la pérdida de la personalidad digital en la supuesta arcadia de la transparencia y participación en las redes sociales. ¿Con qué legitimidad se va a esgrimir en la sociedad digital la bandera de la transparencia y de la verdad, si nuestra memoria no para de cincelar el pasado de cada uno adaptándolo a las necesidades de literarias de reconstrucción de nuestros recuerdos? Nuestro subconsciente, que no cesa en el empeño de protegernos moldea siempre nuestros recuerdos de manera que nuestra propia historia sea metabolizable para uno mismo.

Advertidos de todo lo anterior, aunque quien les habla profesa un optimismo menos contundente que el beneficiario, el Dr. Marco desarrolla su formulación en favor de un nuevo contrato social en el presente contexto histórico, que es el de la quinta revolución tecnológica, que apenas emerge en la actualidad, presidida por la transformación digital. La ecuación formulada en el discurso es ceder parte de nuestra privacidad (datos) a cambio de una tecnología segura, sabedores de que los datos y el *big data* serán el epicentro de los cambios estructurales y sociales que se avecinan.

Y, en este proceso de cambio, el Dr. Marco sugiere que el nuevo contrato social que diseña en su discurso sería una suerte de nuevo objetivo ilustrado para salir de las tinieblas neomedievales en las que vivimos. El pacto social que postula sería equivalente a la luz de la razón frente a la anomia de la superstición que impera hoy en día.

Ciertamente en el discurso el nuevo contrato social es una puesta futurista, pero formulada con lucidez e innovación. Recogiendo todas las doctrinas que intentan formular soluciones utópicas frente al paisaje reinante de distopías. La formulación arranca de un presupuesto, nada más nacer albergamos una personalidad digital que es universal y que requerirá un contrato social que se articula sobre la confianza en el sistema. El sistema a su vez deberá dotarse de una red con un nodo central conectado a todos los miembros de la red. Las intercomunicaciones de un nodo a otro deberán pasar siempre por el nodo central. Aquí se suscita uno de los nudos gordianos del planteamiento del Dr. Marco. En el discurso se apuesta por un nodo central que deberá estar gestionado y presidido por un organismo internacional multilateral, que represente a los Estados, algo así como una formulación futurista de la ONU. Así se dotaría de protección al nodo central y al resto de redes descentralizadas. Y

la apuesta es sugestiva por cuanto en su formulación los ciudadanos ostentarían un derecho primordial al uso de las redes sin una cesión de sus datos. ¿Cómo es posible esta suerte de compromiso equilibrado?: los datos que cada individuo genera nada más nacer se acumularían en una caja fuerte digital especial que estaría tanto en el interior de nuestros sistemas informáticos particulares como de nuestros smartphones. Esta caja fuerte debería ostentar una doble vía de protección, una la que implementemos nosotros mismos sobre nuestro sistema de comunicación y otra la que debe implementar el organismo multilateral que proteja el nodo central. De este modo para utilizar las redes (app, Google etc.) no se producirá la cesión de nuestros datos y mucho menos de forma gratuita como en la actualidad. En el nuevo contrato social las empresas de telecomunicaciones pondrán precio a sus servicios, que los podremos pagar con dinero o bien con nuestros propios datos mediante cesiones individuales y no permanentes. De este modo los datos saldrían temporalmente de nuestra caja digital, con consentimiento expreso, cuando se quiera usar un bien o un servicio. Con esta fórmula el Dr. Marco pretende que los bancos no guarden nuestros registros de ingresos y pagos, del mismo modo que no se podrán crear perfiles de usuario por cuanto tampoco las empresas, por ejemplo, de car sharing o las de comida a domicilio guardarán nuestros datos. Igual ocurrirá si acudimos a Amazon. Y la puesta es audaz, de manera que si utilizamos la tarjeta de crédito expresaremos un consentimiento temporal a que el banco consulte a nuestra caja digital. Se trataría de invertir el proceso tal y como ahora se efectúa. Así, por ejemplo, Amazon nos pedirá permiso para consultar nuestras últimas compras porque no habrá guardado un registro de nuestros movimientos, ese registro solo lo ostentará el titular de los datos.

El ciclo conceptual se cierra con la intervención del Estado con el que mantenemos el contrato social analógico, el Estado con-

sultará nuestros datos de compras, nuestros movimientos de ingresos y gastos en nuestra caja digital. Esto le proporcionará una radiografía tributaria del contribuyente, de modo que si el ciudadano deniega el acceso o comete cualquier infracción, los poderes públicos deberán acudir a los Tribunales para que, formulando solicitud al organismo multilateral centralizado, se autorice el acceso forzoso.

Y la utopía del beneficiario culmina con un futuro en que los ciudadanos tendrían un sueldo mínimo nada más producirse la entrada de nuestros datos en la caja fuerte personal, donde se almacenará nuestra huella dactilar los datos médicos y demás necesidades desde que se produzca el nacimiento del ciudadano. Con esos datos se negociarán ventajas con empresas de todo tipo de productos que pagarán por aquéllos o bien negociarán descuentos a cambio de datos.

En su discurso Francisco Marco señala como uno de los obstáculos para caminar hacia esta cultura del nuevo contrato social la defensa ultranza de la *privacy*. Es decir, la cultura garantista tradicional de defensa de la privacidad sería un obstáculo para alcanzar ese nuevo escenario ilustrado, llegando a señalar que la defensa ultranza del derecho a la *privacy* podría llegar a constituir una nueva inquisición frente a los planteamientos que formula de nuevo compromiso social. Personalmente no creo que el principal enemigo de la puesta que formula el Dr. Marco sea esa cultura garantista. El principal obstáculo para avanzar hacia esas fórmulas de compromiso y de equilibrio, a mi juicio, se sitúa en el poder de las grandes corporaciones que a día de hoy controlan nuestros datos y nuestra vida digital. Las plataformas digitales se han desarrollado en los últimos 25 años bajo el reinado de la anomia, o cuanto menos de la frustrada intervención de los poderes públicos que han fracasado a la hora de imponer un marco jurídico regulativo. Internet nació bajo es-

lógenes de cultura pseudoanarquista o hippie: todos seremos consumidores y productores de información de manera autónoma y libre fuera de la regulación de los Estados. La realidad ha sido otra, los monopolios de las corporaciones digitales que acumulan nuestros datos y los controlan, finalmente han acabado por resultar la verdadera nueva inquisición en un contexto de pérdida de libertades y de auténtico libre desarrollo de la personalidad de los ciudadanos.

Por consiguiente, el reto de futuro es imaginar fórmulas de regulación jurídica de obligado cumplimiento, que fluyan desde entes públicos internacionales, que puedan exigir el obligado cumplimiento de las reglas. Solo así el nuevo contrato social que postula el Dr.Marco será posible y operativo.

La angustia del jurista en la actualidad viene dada por la impotencia a hora de formular soluciones jurídicas frente al desarrollo tecnológico imparable. La nueva revolución digital, que tan bien dibuja el Dr.Marco en su discurso, redobla y multiplica esta angustia del jurista. Esta sensación de impotencia. Y se aportan buenas razones en el discurso de los fracasos de la cultura jurídica de protección de datos y de la última reformulación de los anhelos de intimidad en las Redes sobre la idea de derecho al anonimato en la navegación por las mismas.

Estoy absolutamente de acuerdo con las advertencias que se formulan en el discurso de ingreso a esta Real Academia, si no se propugnan soluciones de futuro. Los datos son el nuevo valor absoluto, como en su día fue el petróleo, como señala Francisco Marco serán el combustible del futuro vertebrador del negocio de las empresas. Si se continúa con la anomia actual los riesgos que derivan del manejo incontrolado de datos son muy graves. Es posible la discriminación predictiva en el sector de la medicina, del empleo y de los seguros; también se atisba un

fenómeno creciente de control gubernamental fuera de los límites propios del Estado de Derecho. Todo esto son grandes peligros que derivan de la pérdida del anonimato. Y sabemos que la revolución tecnológica es imparable, como se señala en el discurso de ingreso se trata de la quinta revolución industrial.

Como antes indiqué, la apuesta de Francisco Marco se ubica en una órbita de optimismo, que el sitúa conceptualmente en una suerte de optimismo racional, tomando las enseñanzas de Pinker. Es cierto que cotizan más al alza los planteamientos pesimistas, son considerados como más serios y moralmente superiores. Parece que la profundidad de la reflexión solo puede venir dada de la mano del pesimismo. Estoy a favor de la superación de este impasse histórico que padecemos. Creo que no podemos seguir operando con modelos racionales e ideológicos que han caducado o que deben caducar. En los últimos años he escrito sobre la necesidad de un pesimismo activo del que habla Alain Minc en su obra “La Nueva Edad Media”. Si se prefiere se trata de un optimismo relativo porque el reto es evitar la caída del progreso, porque es un mito la permanente construcción del mismo. No podemos entender por progreso el desarrollo tecnológico descontrolado e inquisitivo. El compromiso se centra en conservar estables las sociedades. En esa necesidad se inscribe la propuesta de Francisco Marco. Como he escrito en otras ocasiones el pesimismo activo o el optimismo relativo reclama anticipación y lucidez, y como he señalado en otro lugar “su reto es pensar la incertidumbre desde unos postulados mínimos de certeza, sabedores de que no se sale impunemente de varios siglos regidos por el culto al progreso, dando por descontado que el orden iba a reinar eternamente”.

El discurso de ingreso de Francisco Marco se formula con anticipación y lucidez y probablemente el pensador Alain Minc estaría, satisfecho si hoy estuviera aquí escuchando a Francisco Marco.

Acabo ya Sr.Presidente. Hemos escuchado un discurso de ingreso de elevada categoría del que se desprenden conclusiones equilibradas y novedosas, bien articulado y fundamentado en estudios previos del Dr.Marco que a buen seguro van a requerir desarrollos ulteriores y reflexiones en el seno de la Academia.

El Dr. Francisco Marco se ha pronunciado de manera coherente conforme a su pensamiento inscrito en las mejores ideas liberales que dimanen del Estado social de Derecho. Sus formulaciones son bondadosas, pretenden poner coto al autoritarismo, la inquisición y el populismo en las plataformas digitales. La reflexión arranca del reconocimiento de una realidad insatisfactoria, una realidad maquillada y colonizada por las grandes compañías que operan con nuestros datos.

Las aportaciones que realiza el Dr.Marco Fernández, a través de su discurso, constituyen una demostración evidente de los quehaceres que quedan pendientes y que desde el plano jurídico social y político se deben afrontar. Una institución como esta Real Academia Europea de Doctores debe hacerse eco de las necesidades de futuro, deberá desplegar su actividad en búsqueda de fórmulas de equilibrio social como las que sugiere el recipiendario.

La Real Academia Europea de Doctores incorpora a un pensador que realza la institución y suma a la misma un talante de indeclinable compromiso con la misma, un nuevo Académico que aportará frescura intelectual a partir de una experiencia acrisolada.

La Real Academia de Doctores está pues de enhorabuena con el ingreso del Dr.Francisco Marco Fernández a quien felicito con el rigor del solemne acto académico y le doy la bienvenida en mi condición de Académico que contesta su discurso en nombre propio y de todos los presentes; en el plano personal este acto de

ingreso me produce una profunda ilusión, que expreso con emoción contenida al recordar a aquel joven que hace veintisiete años se me acercó con la ilusión de realizar la tesis doctoral.



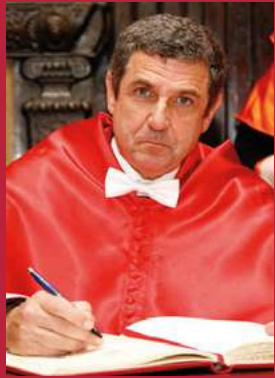
PUBLICACIONES DE LA REAL ACADEMIA
EUROPEA DE DOCTORES

Publicaciones



Revista RAED Tribuna Plural





FERMÍN MORALES PRATS (Barcelona 1957) es Doctor en Derecho por la Universitat de Barcelona (1983). En 1984 le fue concedido el Premio extraordinario de Doctorado, por la Universitat de Barcelona, por la tesis doctoral “La intimidad en el Derecho Penal español” (posteriormente publicada bajo el título “La tutela penal de la intimidad: *privacy* e informática). Desde 1994 es Catedrático de Derecho Penal en la UAB. Con anterioridad fue Catedrático en las Universidades de Cantabria (Santander) y de Lleida. El 15 de Septiembre de 1994 se produce la toma de posesión como Catedrático de la Universidad Autònoma de Barcelona, después de celebrado el pertinente concurso-oposición.

Docente en la UAB, ESADE, Abad Oliba, ISDE, Economist & Jurist School, ICAB así como es ponente en multitud de conferencias y seminarios.

Director de numeras tesis doctorales, ha participado en proyectos de investigación de ámbito nacional e internacional. Investigador en los años 80 y 90 en el Max Planck Institut für ausländisches und internationales Strafrecht (Freiburg. i. Br. Alemania) y en el Institut für Kriminologie und Wirtschaftsstrafrecht (Universität Freiburg i. Br. Alemania), bajo la dirección del Prof. K. Tiedemann.

Es autor de más de setenta publicaciones en el ámbito de la Dogmática del Derecho Penal y de la Política-criminal.

Es codirector de la revista Derecho y Proceso Penal de la editorial Aranzadi.

Abogado en ejercicio.

Nombrado Académico Numerario de la Reial Academia Europea de Doctores en Barcelona el día 5/11/2015 con el discurso de ingreso “La utopía garantista del Derecho Penal en la nueva Edad Media”.



Las imágenes han desplazado a las palabras. Los creadores de internet han conseguido que unas pocas empresas tengan más poder y más dinero que muchos estados simplemente “enganchándonos” a la sencillez de lo visual y a la ilusoria gratuidad. Han conseguido mantenernos frente a la pantalla con trampas psicológicas lo que ha provocado que puedan controlar nuestros movimientos digitales y que nuestra personalidad se disocie.

Es cierto, el futuro ha llegado y ha desdoblado nuestra personalidad jurídica. El nacimiento determina la personalidad y la muerte la extingue; sin embargo, con la amortización de la cuarta revolución industrial, y la quinta a punto de llegar, se atisba la existencia de una doble personalidad en todos los individuos, una analógica y otra digital. Ambas personas, la digital y la analógica, son diferentes lo que ha provocado -y provocará más aún- una dicotomía jurídica, económica, social y psicológica en un mismo individuo. Como se comprueba en este trabajo, esa personalidad digital (identidad digital) no solo se configura con lo que decimos de nosotros mismos, sino que se complementa con lo que los demás pueden recopilar de las pistas (migas de pan) que vamos dejando mientras navegamos. Es lo que se conoce como la paradoja de Pulgarcito. Navegamos y dejamos ir pistas de nuestra identidad digital que alguien agrega y estudia. Y esa identidad digital es cada día más importante.

“El futuro ha llegado y ha desdoblado nuestra personalidad jurídica. ¿Necesitamos un nuevo contrato social?”

Francisco Marco Fernández

1914 - 2022

Colección Real Academia Europea de Doctores