

LA PRIMERA EN EL PELIGRO DE LA PRIVACIDAD: LA UNIÓN EUROPEA Y LA DEFENSA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES

Leonardo Cervera Navas

Discurso de ingreso como Académico Correspondiente en Bruselas, 3 de noviembre 2017

Agradezco a la Academia Malagueña de Ciencias el inmenso honor que me hacen al incorporarme a esta institución que cuenta ya con ciento cuarenta y cinco años de historia, y a los académicos doña Esther Cruces Blanco, don Luis Machuca Santa-Cruz y don Ángel Sánchez Blanco, por proponer mi ingreso. Mi agradecimiento particular al Ilustrísimo señor don Ángel Sánchez Blanco, que fue mi profesor de derecho administrativo en la Facultad de Derecho de Málaga a finales de los ochenta y comienzos de los noventa, y que como promotor de esta iniciativa me recibe hoy acompañado de un grupo de sus alumnos actuales a los que saludo también, animándoles a que perseveren en sus estudios.

He desarrollado la mayor parte de mi carrera profesional en las Instituciones Europeas en Bruselas, donde resido desde hace ya dieciocho años, pero mi vinculación personal y sentimental con la ciudad de Málaga ha permanecido siempre muy firme, como pueden atestiguar los familiares y amigos que me acompañan hoy en este acto. Por ese motivo recibo este nombramiento como Académico correspondiente en Bruselas con tanta ilusión, y desde mis responsabilidades en la Unión Europea, me esforzaré para contribuir a los fines de la Academia reflejados en el artículo 4 de sus estatutos, es decir, la colaboración con las entidades y organismos públicos de la Unión Europea y con otras academias y entidades de similar naturaleza establecidas en Bélgica.

El año 1941, la actriz Greta Garbo rodó su última película. Tenía 36 años y aunque se encontraba en el cénit de su carrera, estaba preocupada por los efectos de la edad y un poco desilusionada por las críticas a su última película, así que dijo: "I want to be left alone", "quiero que me dejen en paz", y se retiró, sin que nadie lograra jamás convencerla para

que volviera a ponerse delante de los focos o conceder una entrevista.



Greta Garbo (1905-1990).

La Garbo no quería estar sola. De hecho, sus biógrafos dan fe de que vivió toda su vida rodeada de infinidad de amigos. Lo que la Garbo quería es que la dejaran en paz, en otras palabras, que respetasen su privacidad.

Durante casi cincuenta años, la actriz vivió en el más completo anonimato, hasta que el año 1990, un paparazzi desalmado la fotografió a las puertas del hospital al que acudía dos veces por semana para hacerse el tratamiento de diálisis. La publicación de la fotografía en las que se veía a la gran diva decrepita, a las puertas de la muerte, provocaron una enorme indignación en todo el mundo como muchos de ustedes seguramente recordarán.

No sólo las celebridades, también las personas corrientes, necesitamos que

se respete nuestra privacidad, la intimidad de nuestros hogares, la confidencialidad de nuestras conversaciones telefónicas o correos electrónicos, el secreto de nuestra ideología política u orientación sexual. El respeto de nuestra privacidad es fundamental porque, aunque a veces nos cueste reconocerlo, los seres humanos somos animales profundamente sociales y, por tanto, nuestro comportamiento está muy influenciado por las opiniones de los demás.

El único comportamiento humano que es verdaderamente libre es el que se hace en privado, lejos de la mirada de los demás. Por eso, por citar un ejemplo, para que un voto pueda considerarse válido, es preciso que sea estrictamente secreto, pues de lo contrario se puede influenciar fácilmente, que es lo que hacen algunas organizaciones que se dicen democráticas pero que buscan siempre el voto público y asambleario.



Cabinas para la votación.

El derecho a la privacidad aparece recogido en el artículo 7 de la carta de los derechos fundamentales de la Unión Europea, que es la constitución con otro nombre que nos hemos dado todos los europeos, y que dice así:

“Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”.

Se trata de un derecho negativo, ya antiguo, recogido en las primeras constituciones liberales del siglo XIX, pero recientemente ha surgido en Europa un derecho a la privacidad más moderno, que no es negativo sino afirmativo, y que está relacionado con la informática y el tratamiento de los datos de las personas con la ayuda de los ordenadores.

El derecho a la protección de datos personales permite a las personas no sólo

protegerse de las miradas de los demás sino decidir y controlar la información personal que compartimos, por decisión propia o por exigencias de la ley, con terceras personas o con la sociedad en general.

Este nuevo derecho aparece recogido en el artículo 8 de la Carta de Derechos Fundamentales y dice así:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Al ser un derecho tan novedoso, los redactores de la vigente constitución española, hace cuarenta años, lo intuían, pero no sabían muy bien como formularlo en nuestra carta magna. Por eso, al final del artículo 18, tras recoger las formulaciones clásicas del derecho a la privacidad (intimidad, hogar, secreto de las comunicaciones, etc.) añadieron la siguiente frase:

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Es decir, lo que hoy conocemos como el derecho a la protección de los datos personales.

Ambos derechos, privacidad y protección de datos, se encuentran al mismo nivel que otros derechos fundamentales de la Unión Europea, como el derecho a la libertad y la seguridad, recogido en el artículo 6, o los derechos a la libertad de expresión y reunión, en los artículos 11 y 12, respectivamente.

Los estadounidenses, que no han incorporado todavía el derecho a la protección de datos a su antigua y venerable constitución, no comprenden muy bien por qué nosotros, los europeos, damos tanta importancia a este derecho, aunque a decir verdad tampoco nosotros entendemos muy bien la importancia que le dan ellos a la famosa segunda enmienda de su constitución, que otorga a cualquier ciudadano estadounidense el derecho sacrosanto a poseer y portar armas.



La bandera europea.

Así pues, mi propósito con esta breve presentación es exponerles, de la manera más amena y entretenida posible:

- a) la grave amenaza que se cierne hoy en día sobre la privacidad de las personas a causa de la vigilancia masiva a las que estamos todos sometidos con la ayuda de la tecnología, y
- b) la respuesta firme de la Unión a esta amenaza, por lo que, parafraseando el lema de nuestra ciudad, podemos decir con orgullo que la Unión Europea es la primera en el peligro de la privacidad.

La siguiente imagen es una de las tarjetas de registro que diseñaron las autoridades nazis a finales de los años 30. Eran tarjetas perforables compatibles con la máquina IBM Hollerith D11, que era una especie de máquina calculadora avanzada que permitía procesar la información contenida en esas tarjetas muy rápidamente, es decir, el precedente directo de los ordenadores.



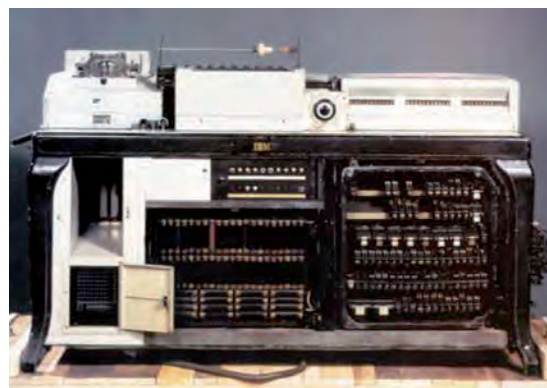
Tarjetas perforadas utilizadas durante el régimen de Hitler.

Las autoridades del Tercer Reich, en su afán totalitario, querían conocer en todo momento donde estaban aquellas personas que ellos consideraban útiles para la guerra, como los hombres en edad militar o los trabajadores cualificados, y dónde estaban aquellos que ellos

consideraban una amenaza para el régimen o inútiles para sus propósitos, y que por tanto había que exterminar, ya fueran enfermos mentales o personas con enfermedades hereditarias, adversarios políticos, gitanos o judíos.

Los nazis se dieron cuenta en seguida que ese control exhaustivo que pretendían era imposible sobre la base de registros tradicionales en libros y en papel y, por tanto, con la ayuda de la sucursal alemana de la compañía estadounidense IBM, desarrollaron un sistema de tarjetas perforadas y distribuyeron miles de pre-computadoras por Alemania, primero, y por los países ocupados después. Así pues, si alguno de ustedes se ha preguntado alguna vez de dónde sacaban los oficiales de la Gestapo sus listas de la muerte, ya tienen la respuesta.

Durante la segunda guerra mundial, sólo en Alemania, había unas dos mil Hollerith D11s, y cada campo de concentración o de exterminio tenía la suya, que se encargaba de procesar la información de los prisioneros que ingresaban en el campo. Algunos criterios de clasificación se pueden considerar más o menos normales tales como el sexo, edad, lugar de nacimiento, profesión, etc., pero hay otros que resultan particularmente dolorosos. Por ejemplo, el código para identificar a las personas con antepasados judíos era el número 8; para los gitanos, el 12; para los homosexuales, el 3, y para los comunistas españoles, el número 6, que era el número que estaba perforado en las fichas de los 142 malagueños que murieron asesinados en el campo de concentración de Mauthausen.



Hollerith D11s, computadora diseñada por Herman Hollerith para procesar los datos de las tarjetas perforadas.

Así pues, las rampas a las cámaras de gas no empezaban cuando los judíos bajaban

de los trenes en Auschwitz o en Treblinka, sino mucho antes, cuando los funcionarios del Departamento de Estadística del Tercer Reich procesaban los datos personales de los alemanes y de las personas residentes en los países ocupados durante la guerra, en busca de sus víctimas.

El presente no se puede entender sin estudiar el pasado y nosotros, los ciudadanos europeos, más de setenta años después del final de la guerra civil española y la Segunda Guerra Mundial, seguimos todavía traumatizados por los cataclismos del siglo XX.

Yo me críe oyendo a mis mayores contar historias de bombardeos, paseillos, maquis en la sierra, cárcel, fusilamientos y exilio, y yo creo que fue por eso por lo que escribí una novela sobre la guerra civil en Málaga, como una especie de exorcismo intelectual para sacar de mi mente y de mi alma los horrores que vivieron mis mayores.

Nosotros los ciudadanos de Europa hemos construido nuestro proyecto común, nuestro proyecto europeo, sobre las ruinas de la segunda guerra mundial y con el recuerdo terrible de las alambradas de espino de los campos de exterminio. Por eso, hemos hecho de la democracia y la defensa de los derechos fundamentales nuestra bandera común durante muchas décadas, y por eso nos preocupa tanto que el estado pueda usar otra vez la informática contras las personas.

Hoy en día, por desgracia, vivimos el resurgir de los nacionalismos y las ideologías excluyentes, con discursos populistas que ofrecen soluciones mágicas a problemas muy complejos, con mentiras y manipulaciones en lo que ya se conoce como la era de la post-verdad y las *fake news* (noticias falsas).



Fake news.

Quizás alguno de ustedes esté pensando ahora mismo que esto que les

dice este conferenciante es interesante pero no se corresponde mucho con el tema de la disertación pero, mucho me temo que sí, que es pertinente, pues si están siguiendo las noticias internacionales estos días habrán oído que existen indicios alarmantes de que la sorprendente victoria de Donald Trump y de los partidarios del Brexit fue posible gracias a la identificación en Internet de los votantes indecisos a los que se logró influenciar con propaganda y noticias falsas en las redes sociales, como la de esa activista catalana que denunciaba en un video que dio la vuelta al mundo que la malvada policía española le había tocado las tetas y le había roto, uno a uno, los cinco dedos de la mano.

Este fenómeno de las *fake news* es ahora mismo uno de los motivos de mayor preocupación para la Unión Europea. Se trata de una estrategia desarrollada por terceros países, Rusia en particular, para desestabilizar nuestras sociedades occidentales, sobre todo durante los procesos electorales.

La estrategia de estos terceros países se ampara en la desconfianza general de la población hacia su clase política y en el hecho constatado de que la mayoría de la gente ya no se informa leyendo los periódicos, cuyos contenidos suelen estar contrastados, aunque a veces, como ha reconocido recientemente el periódico británico *The Guardian* en la crisis catalana, también pueden llegar a ser víctimas de las *fake news*, sino directamente, en las redes sociales.

Con la ayuda de agentes extranjeros que compran publicidad en Facebook o en YouTube, y de *bots*, es decir, robots que se hacen pasar por personas reales en las redes sociales, estas potencias extranjeras inundan nuestros muros en Facebook con mentiras, medias-verdades y propaganda que no nos permite ya distinguir lo que es verdad de lo que es mentira (de ahí el término post-verdad).

Así pues, los muros de Facebook de los alemanes se llenan con videos de inmigrantes invadiendo el país en masa y haciendo desprecio de la cultura alemana; los muros de Facebook de los ingleses se llenan con videos de políticos y funcionarios corruptos de Bruselas, que quieren robar a los ingleses su dinero y su soberanía, y en el caso de España, nuestros muros se llenan con vídeos de catalanes quemando banderas españolas o de españoles robando el dinero

de los catalanes, dependiendo de si el que se conecta a la red social es un catalán o un cordobés.

De esta manera, estos propagadores de noticias falsas consiguen que un votante tradicional de la CDU alemana, un votante conservador, pase a votar a Alternativa para Alemania, que es un partido neo-nazi, o que votantes que hasta hace poco han sido sólo nacionalistas ahora se declaren independentistas. Por tanto, el propósito de estas potencias extranjeras no es ayudar a un político en particular sino desestabilizar nuestras sociedades y crear el caos. De hecho, parece que los mismos agentes rusos que presuntamente ayudaron al presidente Trump a llegar a la Casa Blanca, ahora estarían trabajando en las redes sociales para lograr su caída.

Pero más allá de posibles manipulaciones electorales con ayuda de la tecnología, el problema de la pérdida de la privacidad de las personas a consecuencia de la tecnología va mucho más allá.

Da vértigo comprobar la cantidad de información personal que circula hoy en día por la Red sin control, porque, además, la capacidad de computación y almacenamiento digital de la información se duplica cada dos años de manera exponencial en lo que se conoce como la Ley de Moore. Por explicarlo de una manera gráfica, si en el año 2013 nuestros “coches digitales” tenían capacidad para transportar cinco pasajeros y circular a cien kilómetros por hora, el año 2015 empezaron a circular a doscientos kilómetros por hora y a llevar diez pasajeros, hoy en día circulan ya a cuatrocientos kilómetros por hora con capacidad para llevar a veinte pasajeros, y antes de que termine el siglo, ya estarán circulando a más de mil kilómetros por hora con capacidad para cuarenta pasajeros.

Se calcula que sólo entre el año 2013 y el año 2015, por ejemplo, se creó y se almacenó tanta información en los servidores de Internet como toda la información que había creado la humanidad hasta entonces, desde Altamira hasta nuestros días.



Servidores de almacenamiento de datos de Internet.

Para el año 2020 habrá 6 billones de personas usando teléfonos inteligentes y 50 billones de aparatos conectados a Internet, todos ellos generando y compartiendo información personal sobre todos nosotros. Cada año se vuelcan en la red trillones de fotografías, por ejemplo, como las decenas que tomaremos hoy de este acto con nuestros teléfonos móviles sin ir más lejos.

Toda esta enorme capacidad de procesamiento y almacenamiento es lo que se ha venido en denominar el “big data”. Hay además otra tecnología, la conocida como Internet de las cosas, que significa que ya no tenemos cosas a las que a veces se incorpora un ordenador, sino ordenadores que además sirven para hacer otras cosas, ya sea llamar por teléfono o llevarnos de un lado para otro con cuatro ruedas y un motor. Estas tecnologías tienen un enorme potencial de lograr avances que eran inimaginables hace sólo unos pocos años: pulseras que detectarán la proximidad de una embolia o un infarto, coches que se conducirán solos sin tener jamás accidentes o drones que llevarán la compra a nuestras casas inteligentes.



Teléfonos inteligentes.

Así, en ese futuro tecnológico maravilloso que ya se vislumbra y que nos

van a vender los gigantes del Internet, las persianas de mi habitación se levantarán poco a poco por la mañana para que me despierte sin sobresaltos. Mi asistente personal robotizado (que será una versión avanzada del Siri del teléfono móvil) me pondrá mi música clásica favorita de camino a la ducha, que tendrá el agua a la temperatura que a mí me gusta, y cuando llegue a la cocina, las tostadas y el café ya estarán listos. El frigorífico avisará a Mercadona de que envíe más zumo con un dron, porque ya no queda, y el coche, que se habrá recargado de electricidad durante la noche, me estará esperando a la puerta de mi casa para llevarme de forma segura hasta la oficina, conduciéndose solo por el camino más rápido y evitando los atascos. Cuando regrese a casa del trabajo por la tarde, mi pulsera de fitness me dirá los ejercicios que tengo que hacer para mantenerme en forma, y mi asistente personal me pondrá en la televisión inteligente una película que seguro que me va a gustar, porque mi asistente sabe muy bien todos mis gustos, y si estoy soltero y no tengo hijos, que no es mi caso, me pondrá también en contacto con otras personas del vecindario que sean compatibles con mi orientación sexual y que compartan mis mismas aficiones.

Ese es uno de los futuros posibles, pero también puedo pintarles otro futuro muy diferente, que por supuesto ningún gigante del Internet les venderá jamás. En ese futuro alternativo, cuando me dispongo a salir de mi casa inteligente por la mañana, resulta que no puedo abrir la puerta porque la cerradura electrónica ha sido hackeada. Cuando por fin consigo salir de mi casa saltando por una ventana y lastimándome un tobillo, el coche no arranca porque ha habido un problema con la última actualización del software. Tengo que perder media hora instalando yo mismo la actualización, y cuando el coche arranca finalmente, no me lleva a la oficina por el camino más rápido y directo, sino que da un buen rodeo para pasearme por las calles donde están los bares y las tiendas, a ver si me animo a gastar un poco. Cuando llego por fin a la oficina, me encuentro que mi jefa está muy enfadada porque es la tercera vez que llego tarde en un mes y me da la carta de despedido porque el programa de evaluación de los empleados sabe de mi problema de hipertensión por culpa de mi pulsera de fitness y me ha incluido en la lista de los empleados con una alta probabilidad de padecer diabetes

y sufrir un infarto, por lo que la compañía ha decidido reemplazarme por un chico joven que está más sano que una pera. Cuando llego a mi casa por la noche, me encuentro con el zumo de Mercadona derramado a la puerta de mi casa y un correo electrónico del banco, que ya se ha enterado de que he perdido mi empleo, y ha decidido cancelarme el préstamo que me había dado para comprarme el coche que no arranca por las mañanas, y el asistente que me pone en contacto con otras personas del vecindario con mis mismas aficiones, ya no me encuentra ningún match porque me considera un perdedor.

Esto que les digo les puede parecer a ustedes una exageración, pero piensen por un momento en el rastro digital que estamos dejando inconscientemente en Internet. Ese teléfono inteligente que tenemos todos y que es tan útil porque además de para llamar por teléfono tiene WhatsApp, Google maps, Facebook, Messenger, etc., va grabando en todo momento lo que decimos, con quién hablamos, a donde vamos, a donde entramos o de donde salimos, que vemos en Internet, a qué partido político le damos un "me gusta" en Facebook, qué compramos en Amazon o qué película vemos en Netflix.

De manera inconsciente, estamos generando gigabytes de información sobre nuestros desplazamientos, nuestros hábitos de consumo o nuestras tendencias políticas, que se vuelcan en Internet y se analizan continuamente para propósitos comerciales por las empresas o para propósitos de control o de policía por las autoridades públicas, sobre todo en países totalitarios.

Por eso, los datos personales se han convertido en el oro líquido, en el petróleo del siglo XXI y las empresas que capitalizan con los tratamientos de datos personales valen más hoy en día en bolsa que las petrolíferas. Se calcula que procesando nuestros datos personales y vendiendo esta información a los anunciantes, una compañía como Google puede ingresar alrededor de doscientos euros al año por cada uno de nosotros. No es de extrañar por tanto que "nos regalen" todo en Internet, porque mientras más productos gratuitos utilizamos, más dinero generan estas empresas gracias a nosotros. Así que si alguno de ustedes se ha preguntado por qué en Internet todo es gratis, ya tienen la respuesta.



Empresas multinacionales.

Alguien puede decir que no le importa que Google o Microsoft hagan uso de sus datos personales pues confía en esas compañías y obtiene algo a cambio con productos y servicios gratuitos que son muy útiles, pero aun suponiendo que todos estos datos íntimos que estamos volcando en Internet se usen por esas compañías para propósitos benignos o beneficiosos para nosotros, que ya es mucho suponer, el riesgo de que acaben en manos de hackers o criminales es muy real, y entonces su uso ya no sería para nada benigno o beneficioso para nosotros: estos criminales nos pueden vaciar la cuenta corriente o esperar a nuestro hijo a la puerta del colegio.

Hoy en día vivimos en sociedades democráticas y respetuosas del estado del derecho en las que podemos confiar más o menos que esos datos que generamos inocentemente no se usarán contra nosotros por el estado, pero ¿alguien se ha parado a pensar que pasaría si el día de mañana llegara al poder un gobierno que no es ni democrático ni respetuoso con la ley? Si los nazis hicieron lo que hicieron con calculadoras avanzadas, ¿qué no hubieran hecho con la tecnología que tenemos hoy en día?



Big Brother, personaje de la novela de George Orwell y cofundador del Partido que lo controla todo.

¿Y quién nos garantiza que esas empresas que parecen tan buenas y tan generosas no estarán utilizando todos esos datos a nuestras espaldas para prácticas discriminatorias encubiertas o para subirnos el precio de sus servicios?

Es más, si a las posibilidades del *big data* y el Internet de la cosas, aunamos la inteligencia artificial y el *machine learning*, es decir, computadoras enseñándose unas a otras y haciéndose cada vez más inteligentes sin intervención humana, existe el riesgo real de que nuestras sociedades digitales se encaminen hacia lo que se conoce como la dictadura de los datos, es decir, un mundo en el que las decisiones las tomen las máquinas y no las personas y, lo que es peor, las decisiones no se tomen por lo que diga o haga un determinado sujeto, sino sobre la base de las probabilidades estadísticas de que una determinada persona haga o no haga determinada cosa, ya sea dejar de pagar el recibo de la hipoteca, enfermarse debido a una predisposición genética o cometer un crimen.

En definitiva, poco a poco y sin darnos apenas cuenta, seducidos por los supuestos beneficios de la tecnología, nuestra sociedad podría estar caminando hacia un mundo más oscuro, en el que gobiernos y corporaciones empresariales restrinjan nuestras libertades y derechos con la ayuda de la tecnología, y ese no es el futuro que queremos los europeos para nuestros hijos.



Minority Report, película dirigida por Steven Spielberg, basada en la predicción del futuro.

Es por eso por lo que nosotros, los europeos, hemos considerado a la protección de la privacidad y a la protección de datos como derechos fundamentales en nuestra

Constitución, y es por eso por lo que la Unión Europea se ha convertido en la primera en el peligro de la privacidad en Europa y el resto del mundo.

En menos de seis meses, el día 25 de mayo del año 2018, entrará en vigor el nuevo Reglamento General de Protección de Datos, que es la respuesta de la Unión Europea a la amenaza real que se cierne hoy en día sobre la privacidad de las personas. La respuesta del legislador comunitario, que es el resultado de arduas negociaciones en Bruselas durante años, se basa en tres pilares fundamentales.

1) La ley europea incorpora los estándares de protección de datos más avanzados del mundo. La ley se aplica a todas las empresas que ofrezcan sus productos y servicios a los ciudadanos europeos, con independencia de si la empresa tiene su sede en un país europeo o en un tercer país. Una autoridad independiente de supervisión en cada país de la Unión y una entidad europea de protección de datos, mi empleador, tienen poderes de policía para investigar a instancia de parte o de oficio, cualquier violación de la ley. Si se demuestra que la privacidad de los ciudadanos no ha sido respetada, estas autoridades de supervisión pueden imponer multas millonarias que pueden llegar al 4% de la facturación anual de una empresa a nivel mundial. Son sanciones equivalentes a las que se barajan en el ámbito del derecho de la competencia.

2) El principio de responsabilidad de las empresas (*accountability*). Este principio significa que no basta con dar a los ciudadanos de a pie derechos que a veces pueden ser difíciles o costosos de ejercitar contra los gigantes de Internet. Las compañías que se lucran procesando los datos de las personas tienen la obligación de organizar los tratamientos de datos personales de manera responsable y cuidadosa en todo momento, incluso si nadie se queja o no existe ningún daño demostrable. Para ello la ley crea la nueva figura del responsable de protección de datos dentro de cada compañía, que al igual que el responsable de la seguridad laboral o el médico de empresa, se encargará de velar de que se está respetando la privacidad de los empleados y de los clientes.

3) La responsabilidad de las empresas de garantizar la privacidad de las personas no

es responsabilidad sólo de los abogados sino también de los ingenieros que deben diseñar los productos y servicios que van recoger y compartir nuestros datos personales teniendo en cuenta el impacto que puedan tener sobre la privacidad de las personas. El respeto a la privacidad debe estar por tanto ya presente en el diseño del producto, el servicio (principio de *privacy by design*) y activada por defecto (*privacy by default*).

En definitiva y, en resumen, la respuesta de la Unión Europea al problema de la *datificación* de nuestras sociedades digitales y el peligro que ello supone para la privacidad de las personas se resume muy bien en el considerando cuatro del nuevo reglamento que dice que “el tratamiento de datos personales debe estar concebido para servir a la humanidad”.

No para servir a las empresas para que ganen más dinero o para servir a los gobiernos para limitar nuestros derechos y libertades.

De la misma manera que el crecimiento sin control de las ciudades y de las fábricas en nombre del progreso ha terminado por contaminar el aire hasta hacerlo irrespirable, el tratamiento masivo y sin control de nuestros datos personales terminará por contaminar Internet haciéndolo irrespirable también.



Fábricas emitiendo gases contaminantes.

De la misma manera que el aumento de liquidez a los bancos sin una regulación adecuada, en nombre del crecimiento económico, ha puesto a la humanidad a las puertas de un cataclismo económico, si no nos tomamos muy en serio el tema de la protección de datos, acabaremos presenciando muchos Viernes Negros en Internet, como

los que acabamos de presenciar con la victoria sorprendente de Donald Trump y los partidarios del Brexit, por ejemplo.

En resumidas cuentas y con esto ya termino, enlazando con lo que decía al comienzo de mi intervención cuando me refería a que los ciudadanos europeos habíamos hecho de la defensa de la democracia y de los derechos fundamentales nuestra bandera común, la respuesta de la Unión Europea a los desafíos con los que se enfrenta el mundo hoy en día, ya sea la lucha contra el cambio climático, el problema de los neo-nacionalismos y los populismos, la desbandada de los que viven en los países pobres del sur hacia los países ricos del norte, o los peligros contra las libertades individuales en Internet...



La respuesta a todos estos problemas que amenazan nuestro planeta se puede encontrar en las palabras del preámbulo de la Carta de Derechos Fundamentales de la Unión Europea cuando dice literalmente que:

“La Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y del Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su actuación.”

Así pues, porque la Unión Europea sitúa a la persona en el centro de su actuación, la protección de la privacidad de las personas, garantía de su dignidad y de su libertad, frente a peligros muy reales, es y debe continuar siendo una prioridad y, por eso, los que nos dedicamos a defender este derecho fundamental desde las instituciones europeas seguiremos esforzándonos para que la Unión Europea sea y siga siendo la primera en el peligro de la privacidad.

Agradezco una vez más a la Academia Malagueña de Ciencias por el inmenso honor que me hacen con mi nombramiento como académico correspondiente en Bruselas y a todos ustedes, señoras y señores, por su asistencia a este acto solemne y por su amable atención. Muchas gracias.