ISSN 2704-8012

European Journal of Privacy Law & Technologies

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in Dicember 2019
www.ejplt.tatodpr.eu

European Journal of Privacy Law and Technologies

Avv. Flora Nurcato – Università Suor Orsola Benincasa di Napoli
Ph.D (c) Emiliano Troisi – Università Suor Orsola Benincasa di Napoli
Ph.D (c) Noel Armas Castilla – Universidad de Sevilla
Ph.D. (c) Hans Steege – Gottfried Wilhelm Leibniz Universität Hannove
Ph.D. Sara Saleri – Re:Lab
Avv. Lucio San Marco – Giappichelli Editore

Summary

pag.

Section I: Articles

pag.

Section II: Comments on decisions

INTERNET Y DEMOCRACIA

Tommaso Edoardo Frosini

Resumen

El trabajo estudia la compleja relación entre Internet y la democracia. Comienza recordando que la situación actual recuerda en parte a las cautelas que se manifestaron con la extensión de la televisión. A continuación realiza una reflexión general sobre la crisis de la representación. Luego estudia las posibilidades de mejora que ofrece Internet, pero también las debilidades que conlleva.

Abstract

The work studies the complex relationship between Internet and democracy. It begins explaining that the current situation remembers in part the cautions that were manifested time ago as television spread. Then the paper makes a general reflection on the crisis of representation. Finally it studies the possibilities of improvement that Internet offers, but also the weaknesses that it entails.

Palabras clave: Democracia, Internet, representación.

Key-words: Democracy, Internet, Representation.

1. Internet y liberalismo, antes que democracia

La compleja y complicada relación entre Internet – o bien eso que se manifiesta a través de la Red y en particular de las redes sociales – y la democracia – como el modo y el método con el cual se organiza la sociedad contemporánea –

es ya un tema que suscita gran atención y reflexión por parte de los estudiosos de las ciencias sociales. Divididos entre los que sostienen cómo y por qué Internet puede reforzar la democracia, y los opositores, que ven en Internet una amenaza para la capacidad democrática de los Estados [1].

Me uno a los primeros, porque considero que Internet puede representar una oportunidad para mejorar las formas de la democracia, especialmente en términos de participación política. No creo, sin embargo, que este enfoque deba articularse con exaltaciones acríticas, ignorando las dudas que Internet vierte sobre el funcionamiento de la democracia, como más adelante aclararé.

Pero antes de nada quisiera sentar una premisa general. Considero que el fenómeno de Internet está relacionado más con el liberalismo que con la democracia. Y es que más que condicionar el modo de ser del poder y su declinación en términos de igualdad, destaca la libertad del individuo que se expresa a través de las potencialidades de la llamada "net freedom". Lo que quiere decir sobre todo libertad de expresión como nunca hasta ahora se había podido manifestar en su ejercicio individual. Hoy en día buscar, recibir y difundir sin límites de fronteras informaciones e ideas es verdaderamente posible, gracias a Internet. Y es un logro considerable de la libertad del individuo. [2] Por tanto, Internet, y de manera más general las tecnologías – a mi parecer –, representan un desarrollo de las libertades; o más bien, cómo las libertades han podido crecer notablemente y expandirse hacia nuevas fronteras del actuar humano precisamente gracias al progreso tecnológico. Cierto, las tecnologías no producen sólo libertad; por decirlo de algún modo, la tecnología puede estar al servicio del hombre bueno o malo, del gobernante ilustrado o del déspota. En un Estado constitucional liberal, sin embargo, la dirección política debería estar siempre dirigida hacia intervenciones que den valor y hagan crecer las libertades del individuo, y la utilización de las tecnologías no puede más que ser instrumental a este objetivo. Ciertamente existe un frente adverso: muros virtuales se erigen en lugar de los de piedra. De hecho, existen países (no liberales) que han construido barreras electrónicas para evitar el acceso a parte de la red global, y lo han hecho borrando palabras, nombres y frases clave de los motores de búsqueda, o bien violando la "privacy" de los ciudadanos. [3] Una

[1] Sobre estas cuestiones véase S. Coleman, *Can The Internet Strengthen Democracy?*, Polity Press, Cambridge, 2017.

[2] Expuse profundamente ésta y otras tesis en T.E. Frosini, *Liberté, Egalité, Internet*, Editoriale Scientifica, Nápoles, 2015.

[3] Datos y noticias en E. Schmidt y J. Cohen, La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni, Rizzoli, Milán, 2013, pp. 100 y ss., que hablan de "filtración" y recuerdan cómo China es "el filtrador de informaciones más activo y entusiasta del mundo […] el Great Firewall of China, como se llama al instrumental usado por el gobierno para oscurecer los sitios, es un verdadero guardián de la integridad nacional china".

nueva cortina de información está cubriendo una parte del mundo, donde los videos y los blogs son ya los "samizdat" de nuestros días. Esto, sin embargo, confirma la vocación liberal de Internet, y el miedo que de esta libertad global tienen países intolerantes a la tecnología, pues la viven como una amenaza a su poder absoluto.[4] Basta pensar en la forma en que las tecnologías permitirían, y ya lo hacen, superar al Estado como epicentro único de decisión y poner de esta manera en crisis el concepto de soberanía, tradicionalmente entendido.[5]

He de añadir, así, que se esté desarrollando un nuevo modo de ser del constitucionalismo, el cual se va delineando sobre las robustas y sólidas raíces de la separación de poderes y de la garantía de los derechos con referencia precisamente a la tecnología; o mejor, como manera de dar fuerza y protección a los derechos de libertad del individuo en un contexto social profundamente cambiado por la innovación tecnológica y de sus derivados en el ámbito del Derecho.[6] Se ha hablado también de un "nuevo constitucionalismo, que pone de relieve la materialidad de las situaciones y de las necesidades, que identifica nuevas formas en los vínculos entre las personas y las proyecta en una escala diversa de aquella que hasta ahora habíamos conocido".[7] En este sentido, regresa con fuerza y siempre con mayor convicción la doctrina de la llamada "libertad informática"[8], que con Internet se ha convertido en una exigencia de libertad en sentido activo, no libertad "de" sino libertad "para", que es aquella que se vale

[4] Véase, por ejemplo, el reciente caso de Turquía, donde con la ley de febrero de 2014, el gobierno obliga a los proveedores de servicios de internet a transformarse en agentes de vigilancia y censura realizando remociones y bloques selectivos de contenidos online desagradables y coleccionando todos los datos de los usuarios e incluso sus correos electrónicos: en caso contrario, le revocan la licencia. Cfr. S. Esen y D. Kumcu, "Internet Freedom in Turkey", *Percorsi costituzionali*, núm. 2, 2014, pp. 581 y ss.

[5] Sobre este punto, véase A. Simoncini, "Sovranità e potere nell'era digitale", en T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (coords.), Diritti e libertà in Internet, Le Monnier, Milán, 2017, pp. 19 y ss., que habla del "paradigma tecnológico dominante" y de la "auto-matización como nuevo poder enemigo de la auto-nomía" e invoca el principio de "precaución" constitucional para gobernar la tecnología digital.

[6] Desarrollos en H. Ruiz-Fabri y M. Rosenfels (coords.), Repenser le constitutionnalisme à l'âge de la mondialisation et de la privatisation, Societé de Législation Comparée, París, 2011. Véase también R. Gargarlella (coord.), La Constitución en 2010. 48 propuestas para una sociedad igualitaria, Siglo Veintiuno, México, 2011. He profundizado sobre el tema del constitucionalismo en la sociedad tecnológica en T. E. Frosini, "Costituzionalismo 2.0", Rassegna Parlamentare, núm. 4, 2016, p. 673.

[7] Así, S. Rodotà, Il diritto di avere diritti, Laterza, Roma-Bari, 2012, p. 7.

[8] La doctrina de la libertad informática fue elaborada por V. Frosini, "La protezione della riservatezza nella società informatica", en N. Matteucci (coord.), Privacy e banche dei dati, il Mulino, Bologna, 1981, pp. 37 y ss. (ahora en V. Frosini, Informatica diritto e società, Giuffrè, Milano, 1992, pp. 173 y ss.), y además, con referencia a Internet: V. FROSINI, "L'orizzonte giuridico dell'Internet", Diritto dell'informazione e dell'informatica, núm. 2, 2000, pp. 271 y ss.

de los instrumentos informáticos a fin de proveer y obtener informaciones de cualquier clase. Es el derecho de participación en la sociedad virtual, que ha sido generada con la llegada de las computadoras en la sociedad tecnológica: es una sociedad de componentes móviles y de relaciones dinámicas, y en la que cada individuo participante es soberano en sus decisiones. Nos encontramos, indudablemente, frente a una nueva forma de libertad, que es la de comunicar con quien se quiere, difundiendo las propias opiniones, pensamientos materiales, y la libertad de recibir. Libertad de comunicar, por tanto, como libertad de transmitir y de recibir. Ya no es sólo el ejercicio de la libre manifestación del pensamiento del individuo, sino sobre todo la facultad de éstos de constituir una relación, de transmitir y requerir informaciones, de poder disponer sin límites del nuevo poder de conocimiento conferido por la telemática.

2. Ayer el video-poder; ¿hoy el poder de Internet?

Cursos y recursos históricos, podría decirse. Cuando se rompieron las incrustaciones estatalistas del monopolio estatal televisivo, permitiendo que también los particulares dieran información (y espectáculo) a través de las redes televisivas, y por tanto se diera paso a formas de liberalización del éter, explotó también el tema del llamado "video power". Y, en consecuencia, el temor de que la televisión pudiese convertirse, en manos de particulares, en un instrumento de poder capaz de orientar, o bien manipular, las decisiones políticas de la ciudadanía. Sobre esto escribió un ensayo Giovanni Sartori, y fue uno de los primeros.[9] No niego que la televisión pueda tener capacidades persuasivas, pues es una de sus funciones comerciales (como acontece en el caso de los spots publicitarios), pero hoy, a años de distancia y con la experiencia que hemos adquirido, me parece que puede considerarse significativamente reducido el poder del video, especialmente en las campañas electorales, donde se temía que éstas pudieran facilitar la victoria de "outsiders" improvisados. Dominaba la convicción de que la videopolítica – como argumentaba Sartori – convierte la elección en un elemento altamente fortuito, donde el vencedor es el resultado de un "match" televisivo determinado predominantemente por el aspecto (la cara que gusta) y confiado a flashes, a mensajes persuasivos, de diez segundos. Por ello, entonces, la exigencia de regular la propaganda electoral televisiva reduciéndola en modos y tiempos dictados por la "par condicio". No entro en el fondo, pero con-

[9] G. Sartori, "Videopolitica", Rivista italiana di scienza politica, núm. 2, 1989, pp. 185 y ss. (posteriormente modificado, "Videopotere", Elementi di teoria politica, il Mulino, Bolonia, 1990, p. 303 y ss.); pero véase también F.C. Arterton, Video Politics, Lexington Books, Lexington, 1984.

firmo mis reservas sobre la compresión del "free-market ideas". [10]

Si ayer era el video-poder el que podía minar los fundamentos de la democracia, según una opinión que en esa época se había difundido, hoy las mismas críticas y reservas se dirigen al llamado "Internet power". Ésta es la razón por la que he hablado de cursos y recursos históricos. De hecho, creo que también el temor de una posible dictadura de la web es excesiva, y se reduce, como en el caso de la televisión, a un miedo poco fundado. Por el contrario, la política, o de manera más general las formas en que se aplican los procedimientos democráticos, podría salir reforzada, revigorizada y relanzada.

Antes de ver cómo Internet puede reforzar los modos y las formas de la democracia, creo que es oportuno un breve razonamiento sobre la representación democrática hoy, propedéutico en algunos aspectos precisamente al posible soporte de la web a las democracias febriles. Es necesario partir de un dato fáctico, que es la crisis de la representación política que existe en numerosas democracias contemporáneas.

3. La crisis de la representación como crisis del representado

Es cierto que ha entrado en crisis ese modo tradicional de ser de la representación política: es decir, el mandato para representar a la nación, la responsabilidad atribuida a quien representa, los partidos políticos como asociaciones que representan al electorado, el ejercicio de la función legislativa como tarea primaria de las asambleas representativas, y así también la función de control. Es más, la crisis de la representación también está determinada por la dificultad de encontrar un equilibrio, o mejor dicho una síntesis entre representar y gobernar. [11] Y por tanto al respecto de qué fórmula electoral y de gobierno se haya de adoptar para no comprimir la representación, pero al mismo tiempo valorar la gobernabilidad. De hecho, representar y gobernar es la difícil cuestión sobre la que se mueven las formas de gobierno de las democracias modernas. [12]

La crisis de la representación es también así crisis del representado, pues ha perdido sus referencias políticas e institucionales. Y esto ya sea por la licuefacción de los partidos, que cada vez sirven menos como puente entre la sociedad

[10] Reservas que formulé en un ya lejano escrito mío: T.E. Frosini, "Il decreto legge sulla par condicio nella forma di governo in transizione", en F. Modugno (coord.), *Par condicio e Costituzione*, Giuffrè, Milán, 1997.

[11] Discuto los términos del problema en T.E. Frosini, "Governare è meglio che rappresentare?", *Rassegna Parlamentare*, núm. 1, 2012, p. 7 y ss.

[12] Cfr. T.E. Frosini, *Constitución, democracia y estado de derecho*, Ediciones Olejnik, Santiago de Chile, 2017, *passim*.

política y la sociedad civil (como un tiempo se decía); o por la pérdida de centralidad del Parlamento, como órgano que ya no decide; o incluso, por la desaparición de la relación entre representante y territorio, y por tanto la presencia del elegido como expresión de un colegio electoral. Además, la representación política ha abdicado en favor de otras formas representativas: las de los intereses, a través de los lobbies; las territoriales, en virtud de una acentuación de la descentralización política y administrativa; las de género, que empujan hacia una representación paritaria forzada a través de leyes y normas constitucionales. [13]

La representación, por tanto, se ha parcelado como consecuencia de la acentuación del pluralismo social que parece ya no poder comprimirse sólo en el perímetro parlamentario. Está en crisis la delegación para tomar decisiones: [14] no puede sustentarse con base en una renovada valoración del principio constitucional de soberanía popular, sino más que nada sobre una (todavía) confusa forma de intervencionismo directo, que quisiera encontrar en la web su capacidad de decisión. Y es así que, en cambio, se manifieste, de manera explícita, la crisis del representado, de aquel que busca en otro lugar forma y sustancia para expresar su pensamiento y verlo resuelto en acción, descartando la opción tradicional de la representación política a través del voto, que asume efectividad con el principio mayoritario.

Pero todavía hay más: está en crisis incluso el concepto de soberanía, porque se considera un principio que puede reducirse a un fuerte arbitrio, enemigo del Derecho. [15] Se sostiene que sólo existe el constitucionalismo de los derechos, capaz de purificar la política normativizándola. Otra cuestión, en cambio, tiene que ver con el contraste, siempre más radical, entre el contexto actual de los ordenamientos democráticos y la dimensión global del mercado y de las finanzas, que condicionan las políticas públicas. El paradigma de la soberanía, al que la práctica de la democracia ha estado hasta ahora ligada, ha sido puesta en crisis por una "governance" mundial, que hace referencia a grupos de interés de ca-

[13] Para una serie de consideraciones, R. Orrù, F. Bonini, A. Ciammariconi (coords.), "La rappresentanza in questione", *Giornate di Diritto e Storia costituzionale "Atelier 4 luglio – G.G. Floridia"*, Nápoles, 2016. Véase también el volumen: C. Bassu y G.G. Carboni, *Rappresentanza e globalizzazione*, Turín, 2016, que se origina por el Congreso de la Associazione Dpce, que tuvo lugar en Sassari el 16 de octubre de 2016, y que contiene diversas contribuciones, que tratan las dimensiones de la relación entre representación y globalización. Se reenvía también a la parte monográfica, con numerosas e interesantes contribuciones, dedicada a "Rappresentanza senza populismo", de *Percorsi costituzionali*, núm. 1, 2017.

[14] Sobre este tema, véase A. Schiavone, Non ti delego, Rizzoli, Milán, 2013.

[15] Al respecto véase el interesante estudio de S. Sassi, "Crisi della sovranità e diritto transnazionale", *Percorsi costituzionali*, núm. 1, 2017, pp. 247 y ss.

rácter no electivo, y por tanto sin legitimación democrática. [16] En este sentido, se hace referencia a la arena global de las organizaciones y de los reguladores internacionales, los cuales interactúan entre ellos, y entre ellos y los particulares, a través de un complejo sistema de reglas y de normas, provocando el riesgo del advenimiento de una "tecnocracia global", de la que ha hablado Shapiro. [17]

Las instituciones de la democracia se han debido enfrentar con la necesidad de gobernar dinámicas sociales rápidamente cambiantes y cada vez más complejas como consecuencia del surgimiento de los procesos de globalización y de la explosión de la revolución tecnológica.

4. Internet y la nueva democracia de masas

La revolución tecnológica ha operado con fuerza sobre la organización política de la sociedad occidental, y lo hará incluso más en los años por venir. Ha creado las condiciones para que se formara una nueva democracia de masas, como ha sido claramente definida, [18] distinta y distante de los regímenes de masas de la primera mitad del siglo XX, en los cuales el individuo permanecía en una sujeción psicológica receptiva y pasiva con una total obnubilación de las libertades personales. Esas mismas libertades que, en cambio, se exaltan y valoran en la nueva democracia de masas, "no es sin embargo un destino fatal e irreversible de la sociedad moderna. Ésta es sólo una directriz de marcha de la humanidad, caracterizada por la huella de la civilización tecnológica que le imprime el procedimiento […] En ella se realiza con aparente paradoja una nueva forma de libertad individual, un crecimiento de la sociabilidad humana que se ha crecido en el amplio horizonte del nuevo circuito de las informaciones, una potenciación, por tanto, de la energía intelectual y operativo del individuo que vive en la comunidad". [19]

La libertad informática no se agota, sin embargo, en la (renovada) dimensión de la comunicación y de la información. Ésta comprende también la libertad política y la organización institucional. A través de la tecnología cambian siempre en mayor medida los arreglos institucionales conocidos y la forma en que el proceso democrático es influenciado profundamente por la manera en que circu-

[16] Sobre este punto, la contribución de G. Cerrina Reroni, "Organismi sovranazionali e legittimazione democratica. Spunti per una riflessione", en C. Bassu y G.G. Carboni, *op. cit.*, pp. 45 y ss.

[17] M. Shapiro, "Deliberative, Independent Technocracy v. Democratic Politics: Will the Globe Echo the UE?", *Law&Contemporary Problems*, 2005, pp. 241 y ss.

[18] Así, V. Frosini, *La democracia nel XXI secolo*, Liberilibri, Macerata, 2010, pp. 23 y ss.

[19] V. Frosini, *La democracia nel XXI secolo*, *op. cit*, p. 34.

lan las informaciones, ya que la disponibilidad de éstas por parte de todos los ciudadanos se presenta como un prerrequisito del proceso. La libre circulación de la información puede producir la formación de una conciencia civil y política más informada mediante una llamada a la capacidad de juicio del ciudadano, que ya no es episódica, sino que más bien se ha vuelto parte de un circuito comunitario de información y de responsabilidad. La democracia, y su forma, se plantea de manera diversa a la de los siglos precedentes: cambian los significados de representación y de soberanía, avanza una nueva democracia de masas, que rompe los círculos cerrados de las élites en el poder, obligando a los representantes de la voluntad popular, por decirlo así, a bajar a la plaza telemática y a confrontarse directamente con los representantes, en las nuevas formas asumidas por la tecnopolítica.[20] La nueva democracia ha recibido ya diversas denominaciones: democracia "electrónica" (pero este término define el instrumento y no al agente); "virtual" (pero de esta manera la indicación política resulta debilitada); "continua" (por su carácter de referéndum perenne); o bien "nueva democracia de masas" (con referencia a la antigua democracia directa).[21] Esta ha recibido valoraciones opuestas, dividiéndose sus intérpretes en dos grupos, los que la sostienen y sus detractores, y divididos sobre la respuesta a la cuestión de fondo, que puede ser formulada en los siguientes términos: ¿el impacto político de las tecnologías informáticas sobre los frágiles sistemas complejos que son las democracias contemporáneas favorecería la construcción de un ágora o de totalitarismo electrónicos? La dialéctica de los juicios sobre la nueva forma de democracia está, sin embargo, fundada en un presupuesto común de discusión: la superación de la actual democracia de tipo representativo-parlamentaria.[22]

---

[20] Sobre esta cuestión, véase S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997; S. Rodotà, "Libertà, opportunità, democrazia e informazione", en "Internet e Privacy: quali regole?", Actos del congreso organizado por el Garante para la protección de datos personales, Roma, 1998, pp. 12 y ss. El cual, al referirse a la Internet, la define como "una forma que la democracia puede asumir, y una oportunidad para reforzar la declinante participación política. Es un modo para modificar los procesos de decisión democrática".

[21] Sobre las diversas definiciones citadas en el texto, véanse en ese orden los siguientes estudios: L.K. Grossman, *The Electronic Republic, Reshaping Democracy in the Information Age*, Viking, Nueva York, 1995; L. Scheer, *La democrazia virtuale*, trad. G. Comerio, Costa & Nolan, Génova, 1997; D. Rousseau (dir.), *La démocratie continue*, Lgdj, París-Bruselas, 1995; V. Frosini, *La democrazia nel XXI secolo*, Ideazione, Roma, 1997 (V. Frosini, "La democrazia informatica non è autoritaria, ma di massa", *Telèma*, núm. 14, 1998, pp. 105 y ss.).

[22] Véase I. Budge, *The new Challenge of Direct Democracy*, Polity, Cambridge, 1996, el cual sostiene que el nuevo desafío de la democracia directa dará a los ciudadanos los instrumentos informativos y formativos para una participación consciente en la vida política de la comunidad a la cual pertenecen y llevará también a revitalizar los organismos representativos. Véanse también las

También la llamada democracia electoral – aquella fundada en el mecanismo del voto – ya está sufriendo transformaciones después del desarrollo tecnológico de las sociedades contemporáneas. Por ahora, las transformaciones están relacionadas esencialmente con las técnicas de votación, o bien con la forma en que se vota. La papeleta electoral en papel sobre la que se coloca la propia elección política está próxima a ser dejada de lado. Está ya en fase de utilización en diversas partes del mundo [23] el llamado voto electrónico, que prevé la emisión del voto a través de computadoras. En lugar de poner una marca con un lápiz sobre la papeleta electoral, se podrá oprimir una tecla de la computadora, en cuya pantalla se reproduciría la papeleta electoral, y expresar así el voto y la propia preferencia política. Esta técnica de votación – que es simple de realizar en el caso del voto para los referendos, debiendo elegir sólo entre un "sí" o un "no" – permitiría tener los resultados electorales en un brevísimo tiempo una vez que se hayan cerrado las votaciones, y evitar los agotadores cálculos y escrutinios que, por otro lado, siempre están sujetos al riesgo de fraudes electorales. La votación "online" podría también ser utilizada, con simplificación y racionalización, para las primarias con las que se seleccionan a los candidatos a los cargos de elección popular. En lugar de mesas dispersas por todo el territorio para la emisión del voto, con mayor riesgo de fraude o líos en el cómputo final, bastaría una organización en la web, donde pudieran recogerse "online" los sufragios de quienes quisieran expresar su preferencia por las candidaturas.

Pero los escenarios futuros de la democracia electoral no paran con el voto electrónico. De hecho, se podría también prever el voto a través de la propia computadora de casa, o incluso a través del televisor con auxilio del control remoto. Ciertamente, esta técnica de votación casera si bien por un lado podría reducir el abstencionismo (así como los gastos electorales), por otro lado, impondría la fijación de toda una serie de garantías (incluso de carácter técnico) para proteger la libertad de voto. Libertades que también – y quizá, sobre todo – en la época de la política tecnologizada y globalizada permanece siempre como un valor constitucional al que se debe proteger celosamente. Pero frente al futuro debemos mostrarnos optimistas y apostar por un renovado progreso de la civilización, dando la bienvenida a la nueva democracia tecnológica del siglo XXI, que se funda en la libre iniciativa individual, en la responsabilidad del ciudadano como persona y en su facultad de elección y de decisión. El voto indivi-

críticas y censuras de E. Morozov, *L'ingenuità della rete. Il lato oscuro della libertà in Internet*, trad. M. Renda y F. B. Ardizzoia, Codice edizioni, Turín, 2011. Con consideraciones en claroscuro, M. Ainis, "Democrazia digitale", *Rassegna Parlamentare*, núm. 2, 2013, pp. 263 y ss.

[23] Sobre la difusión del voto electrónico en el mundo, véase L. Trucco, "Il voto elettronico nel quadro della democracia digitale", en T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (coords.), *op. cit*., pp. 427 y ss.

dual se protege y potencia en su disposición telemática, que elimina las manipulaciones, los errores y los fraudes de los sistemas en papel, que permite una posibilidad de elección con el voto inconexo, alternativo o de reserva, que puede ser controlado y calculado con la ayuda de una computadora. Es una democracia no delegante sino participativa, que manifiesta una nueva forma de libertad marcada por la participación del ciudadano en la vida de la colectividad en forma de participación en el poder político. Nace de esta manera una "república libre de la información automatizada [que] equivale, por su funcionalidad de comunicación y por tanto también de sugerencias, revelaciones, acuerdos y delegaciones, a una nueva forma democrática de sociedad que instaura las condiciones técnicas para la puesta en práctica de un régimen político de la democracia de masas". [24]

5. Reforzar la participación política a través de Internet

Y llegamos al punto decisivo: ¿puede Internet reforzar la democracia? [25] Hasta ahora creo haber dado una respuesta sin duda positiva. Ahora intentaré explicar cómo y por qué, para posteriormente desarrollar algunas observaciones conclusivas sobre algunas reservas que de cualquier forma deben ser tomadas en cuenta respecto al tema planteado en la pregunta inicial.

Si la democracia debe ser (también) participación eficaz y efectiva en las decisiones públicas por parte de la ciudadanía, [26] entonces creo que Internet puede contribuir de manera importante en su realización. ¿Cómo? A través de la posibilidad que ofrece la red de promover, mejorar y expandir formas de democracia directa – como "town-hall meeting", "consensus conference", referéndum e iniciativas populares – y de democracia indirecta para el trámite de funciones informativas y de "feedback" populares.

No faltan así distintas experiencias en diversos países, que se van consolidando siempre en mayor medida. La más relevante es la que se presentó en Islandia, donde se procedió, entre abril y julio de 2011, a una especie de participación electrónica en el proceso de revisión constitucional ("web-designed Constitution"), a través de la consulta online, involucrándose a los trescientos mil habitantes de la isla a través de las redes sociales masivas, como Facebook y

[24] Así V. Frosini, *La democrazia nel XXI secolo*, *op. cit.*, p. 33.

[25] Para emplear la pregunta que se plantea S. Coleman, *Can The Internet Strengthen Democracy?*, *op. cit.*

[26] Sobre este tema, véase S. Rodríguez, *Rappresentanza democratica e strumenti di partecipazione. Esperienze di diritto comparato*, Editoriale Scientifica, Nápoles, 2017.

Twitter.[27] Se procedió entonces a un "constitutional crowdsourcing", que produjo cerca de tres mil seiscientos comentarios para un total de trescientas sesenta propuestas. El resultado de este proceso participativo fue aprobado posteriormente por una grandísima mayoría a través de un referéndum, que se llevó a cabo en octubre de 2012, pero que posteriormente se volvió vano por la victoria electoral, en el 2013, de la mayoría de los opositores de la nueva Constitución.

El ejemplo islandés es uno de los más llamativos en los términos de modificación de la Constitución. Otros ejemplos, más difundidos, son los que conciernen medidas legislativas o bien administrativas. Como en Finlandia, donde, a partir del 2012, está activa una plataforma digital "Open Ministry", que permite a los ciudadanos presentar online propuestas de iniciativa parlamentaria o comentarios sobre las leyes en discusión ("crowdsourced law-making system"). Otros ejemplos se podrían referir "Around the World", y también en Italia a nivel regional como en el caso de la Toscana, con el "electronic Town Meeting". En suma, con estas nuevas formas de participación directa en las decisiones de política pública, de las comunidades virtuales que se agregan en Red hasta las deliberaciones cuya decisión está precedida por una amplia discusión "online", el objetivo es "transformar al ciudadano de espectador en actor".[28]

Ciertamente, una precondición para el éxito de la participación de los ciudadanos a través del uso de Internet ("netizenship", como contracción entre "net" y "citizenship"), es el derecho de acceso a Internet. El acceso a Internet constituye el modo con el cual el sujeto se relaciona con los poderes públicos, y por tanto ejerce sus derechos de ciudadanía. Negar el acceso a Internet, o bien hacerlo costoso y en consecuencia exclusivo, significa imposibilitar el ejercicio de la mayor parte de los derechos de ciudadanía. El derecho de acceso a Internet es un tema sobre el cual insisto desde hace ya tiempo, y por tanto reenvío a lo que se ha escrito.[29]

Otras dos palabras finales sobre la acentuación de las formas participativas políticas a través de Internet: el referéndum y el "recall". En el primer caso está claro que puede ser activado en Red en forma continua, sin formalidades procedimentales ni límites en su objeto. De esa manera, sin embargo, más que referéndum, que tiene y no puede no tener una dimensión constitucional y legislativa, se trataría de una forma de sondeo, o bien una manera con la cual la ciudadanía sería llamada (¿por quién? este es el problema) a expresarse sobre algunos

[27] H. Landemore, "Inclusive Constitution-Making: The Icelandic Experiment", *The Journal of Political Philosophy*, núm. 2, 2015, pp. 166 y ss.

[28] Así, M. Ainis, *op. cit.*, p. 271.

[29] Cfr. T.E. Frosini, "Il diritto costituzionale di accesso a Internet", *Rivista Associazione dei Costituzionalisti*, núm 1, 2011. Por último, T.E. Frosini, "Il diritto di accesso a Internet", en T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (coords.), *op. cit.*, pp. 41 y ss.

temas de interés público. Sin ningún vínculo jurídico con el resultado, si acaso se trataría de una propuesta persuasiva sobre la utilidad o no de asumir esa medida objeto de la pregunta en la Web. En el fondo, los ejemplos que he referido en primer término se apegan a este tipo de mecanismo. Temer la avanzada de los llamados referendos en Red, que puedan poner en riesgo el sistema de la representación política, me parece excesivo. Y, de cualquier forma, nos guste o no, se trata de un aumento de la dosis de democracia de la ciudadanía, que de esta manera se involucra en mayor medida, incluso en términos consultivos, en las decisiones que le conciernen directamente. Es demasiado elitista sostener que de esa manera se extiende la competencia para decidir a un número creciente de incompetentes, admitiendo sin ambages que en las oficinas en que se toman las decisiones legislativas están sentadas personas competentes.

Otra cuestión es el "recall", o bien el voto para revocar a alguien electo, sea presidente o parlamentario. La institución es conocida y difundida en diversas partes del mundo: en algunos Estados de Norteamérica y en algunos países de Sudamérica. [30] Es evidente que la Web simplificaría, y por mucho, los procedimientos para activar la revocación. Bastaría un clic para decidir si destituir o no a la persona electa. Cierto es que el "recall" puede funcionar donde se da una elección mediante sufragio universal del Presidente (como en el caso de Venezuela, donde Chávez fue sometido, sin éxito, a "recall") o del Gobernador (como en el caso de California donde, con el voto popular, fue destituido Gray Davis, a sólo once meses de la elección). [31] Y se pueden estudiar modos y métodos de la revocación en un sistema de elección con colegio uninominal. Salvo verificar su compatibilidad con la prohibición de mandato imperativo, que es aún uno de los baluartes de la democracia parlamentaria. [32] De hecho, el mandato vinculante es compatible con la Red, pero incompatible con las instituciones representativas.

6. La democracia en Internet y sus críticos

Existe alguna espina en la rosa de la democracia en Internet y, por tanto, es necesario manejarla con cuidado para evitar pincharse.

Se sostiene que el exceso de intervencionismo en la Red puede debilitar las

[30] Sobre los cuales, véase S. Rodríguez, *op. cit.*, pp. 86 y ss.

[31] Cfr. A. De Petris, "Da "We the people" a "Hasta la vista, Davis!": origini, evoluzione e profili di costituzionalità del recall negli ordinamenti degli Stati Uniti", *Diritto pubblico comparato ed europeo*, núm. 4, 2004, pp. 1793 y ss.

[32] Para los términos de la cuestión, véase R. Scarciglia, *Il divieto di mandato imperativo. Contributo a uno studio di diritto comparato*, Cedam, Padua, 2005.

instituciones representativas, que corren el riesgo de ser sometidas a los deseos del "Internet people". Y que por tanto los partidos políticos atenuarían su alcance constitucional por estar sobrepasados por la movilización "online". Hipótesis ciertamente sugestivas; pero se trata de cualquier manera de hipótesis, que deben verificarse. Diría que depende de nosotros y del uso que hagamos de ellas. Depende de la responsabilidad de los gobernantes y de la de los gobernados. Y, de cualquier forma, el momento decisional es siempre el voto, que determina las decisiones de dirección política las cuales permanecen confiadas a la mayoría parlamentaria y a su gobierno. Imaginar que todo esto pueda ser borrado de la Red y de sus aplicaciones a los procesos decisionales, quiere decir imaginar el fin del constitucionalismo. La red, entonces, podrá servir, en positivo, para aumentar el nivel de participación política de los ciudadanos, a través del pluralismo de las informaciones y el intercambio de las mismas entre ciudadanos y entre éstos y los representantes de las instituciones y de las administraciones. Cierto, la Red podrá, en negativo, si se usa mal y con intenciones demoledoras, debilitar el papel de los partidos, transformándolos en meros lugares de recolección de las propuestas presentadas y compartidas por la Red. Esto, sin embargo, depende de la rebelión de las masas frente a la partidocracia y a la omnipresencia de los partidos y al monopolio político de los mismos. Toca entonces a los partidos saber hacerse más ligeros y menos tentaculares. Quizá, pienso en Italia, a través de una ley que los regule y circunscriba su perímetro de competencia e intervención pública. [33]

Se ha señalado correctamente, que "A pesar de ello, Internet ya ha modificado la percepción de la democracia […] ha cambiado la opinión pública, corrigiendo la manera en que se forman tanto los juicios como las expectativas […] los ciudadanos tienden a volverse más exigentes hacia sus gobiernos […]. Ha reforzado los poderes de control de los electores sobre los electos, pero ha también multiplicado su capacidad de iniciativa, hasta transformar – a veces – a cada individuo en un legislador". [34]

Otra (pequeña) espina en la rosa de la democracia en Internet: la violación del secreto del voto. Esto dependería de los "likes" que demos en las redes sociales, como por ejemplo Facebook o Twitter. [35] Porque cada "like" que dejamos en las redes sociales sería una pieza en un censo voluntario de masas, que terminaría por ofrecer oportunidades y poderes a quien quiere orientar las opi-

[33] He discutido este tema en T.E. Frosini, *Forme di governo e partecipazione popolare*, Giappichelli, Turín, 2008, pp. 363 y ss.

[34] Así, M. Ainis, *op. cit.*, p. 276.

[35] Cfr. S. Kuper, "How Facebook is changing democracy", en "Financial Times", de 15 de junio de 2017.

niones. Estudios conducidos por psicólogos, además, sostienen que bastan sesenta y ocho "likes" de un usuario de Facebook para identificar el color de su piel (con una precisión del 95%), la orientación sexual (88%) y la política (85%). De estos estudios nacieron sociedades de investigación como Cambridge Analytica, las cuales observando y monitoreando las páginas de Facebook por ejemplo en enero, son capaces de prever la forma en que votarás en noviembre. Si las opiniones políticas son conocidas por Facebook, el voto ya no es un secreto. Pero no deja de ser una situación similar a la de los militantes o a la de quien escribe un blog político. No obstante además está siempre la autodeterminación del individuo: si le da "likes" a sus preferencias políticas sabe bien que de esta forma hará conocer a terceros su orientación electoral.

Aún otra (pequeña) espina, que puede pinchar el correcto funcionamiento de la democracia en Internet. Se trata de las llamadas "fake news": es decir de las noticias falsas y tendenciosas, que circulan en Internet y que podrían engañar al consumidor, o bien informar de manera incorrecta y mendaz al ciudadano. Se han señalado incluso riesgos para la democracia y se ha querido someter Internet a reglas de garantía sobre la calidad de las noticias, quizá certificadas por una Autoridad independiente. Expreso mi desacuerdo con esta hipótesis. Las noticias falsas siempre han existido (y existirán) en todos los sectores de la comunicación pública y privada, en la prensa y en la red. En esta última, además, ha de tenerse en cuenta teniendo en cuenta que se amplía la libertad de expresión, que permite mayor transparencia y por tanto permite revelar en mayor medida la verdad contra toda censura. En la red existe concurrencia y pluralismo, en el ámbito de la oferta de informaciones. [36] Sobre este punto ayudan las palabras del juez Oliver W. Holmes, en el famoso voto particular del caso Abrams vs. United States (1919):

"el bien supremo se logra mejor a través del libre comercio de las ideas, que la mejor prueba de la verdad es la capacidad del pensamiento para hacerse aceptar en la competencia del mercado y que la verdad es la única base sobre la cual nuestros deseos pueden ser seguramente realizados". [37]

Finalmente, la gran espina que puede verdaderamente herir la democracia en Internet. Es la llamada democracia económica. [38] Se trata de la concentración de mercado por parte de algunas grandes empresas que operan en Internet: Google, Facebook y Amazon. La primera, Google, domina su sector con una cuota de

[36] Sobre este punto, F. Donati, "Il principio del pluralismo delle fonti informative al tempo di Internet"; O. Pollicino, "Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider", ambos en *Percorsi costituzionali*, núm 1, 2014, pp. 31 y ss., y pp. 45 y ss.

[37] O.W. Holmes, Opinioni dissenzienti, Giuffrè, Milano, 1975, p. 105.

[38] Sobre la cual, véase E.C. Raffiotta, "Libertà economiche e Internet", en T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (coords.), *op. cit*., pp. 413 y ss.

mercado del 88% en el "search advertising" (publicidad en motores de búsqueda); la segunda, Facebook (y sus subsidiarias: Instagram, WhatsApp y Messenger) posee el 77% del tráfico de las redes sociales en dispositivos móviles y, finalmente, la tercera, Amazon, tiene una cuota del 74% en el mercado de e-books. En términos económicos clásicos, las tres son monopolios. Por tanto, existe un serio problema de privación de la libre concurrencia, que limita la esencia de la democracia liberal, a través del abuso de posición dominante y de la dependencia económica. No es, sin embargo, un problema de antitrust, que por otra parte ha hecho que se escuche, aunque sea débilmente, su voz a través de la Autoridad garante europea y la Comisión europea, como en los casos de Microsoft y Google, poniendo en duda que algunas prácticas comerciales (de Google, en particular) puedan ser consideradas vulneraciones del artículo 102 del tratado sobre el funcionamiento de la Unión Europea y del artículo 54 del acuerdo SEE. [39]

Como decía, no es sólo un problema de antitrust. Desde el punto de vista democrático se pueden temer riesgos de un poder económico tan fuerte que pueda condicionar no sólo y no tanto el mercado económico, sino sobre todo el mercado de las ideas. Que podría ser condicionado por las decisiones impuestas por las grandes empresas de Internet, que apuntarían también a lograr un sistema más favorable a sus intereses económicos.

Es deseable, por tanto, una mayor concurrencia en el sector de Internet, permitiendo a otros sujetos entrar en el mercado sin correr el riesgo de ser aplastados por las grandes empresas, que operan como si fueran un régimen monopolista. Como escribía Louis D. Brandeis antes de ser nombrado por Woodrow Wilson juez de la Suprema Corte: "en una sociedad democrática, la existencia de grandes centros de poder privados es peligrosa para la vitalidad de un pueblo libre". [40]

Ampliar, agrandar, expandir la oferta de y en Internet, para intensificar el pluralismo de las informaciones, de las opiniones y de las ideas. También así se podrá consolidar Internet como instrumento al servicio de la democracia y de las libertades.

---

[39] Me refiero al caso Microsoft, sobre el que puede verse A. Giannaccari, "La concentrazione Microsoft-Skype (vs Facebook-WhatsApp?). Ovvero una guerra per bande alle spalle delle Telcos", *Mercato Concorrenza Regole*, núm. 1, 2014, pp. 139 y ss. Véase también A. Giannaccari, "Apple, Amazon e gli e-book: Una storia illecita, pro-competitiva", *Mercato Concorrenza Regole*, núm. 1, 2016, pp. 79 y ss. Con referencia al caso Google, véase V. Comandini, "Google e i mercati dei servizi di ricerca su Internet", *Mercato Concorrenza Regole*, núm. 3, 2013, pp. 541 y ss.

[40] Cfr. M. I. Urofsky, *Louis D. Brandeis: a Life*, Schocken Books, Nueva York, 2012.

RISERVATEZZA E OBLIO: DIRITTI DEI MINORI E SERVIZI DELLA SOCIETÀ DELL'INFORMAZIONE

Fausta Scia

Abstract

Traendo spunto dal d.lgs. n. 101/2018 – recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" – nel presente lavoro ci si è soffermati sulla delicata questione concernente la portata della tutela che il legislatore, sia europeo, sia nazionale, ha inteso riservare al diritto del minore alla protezione dei propri dati personali in relazione ai servizi della società dell'informazione.

Key-words: Minors, Right to be forgotten, ICT

1. Le questioni

Tra i diritti della personalità, i diritti all'onore e alla reputazione (artt. 594, 595 c.p. e artt. 2 e 3 Cost.) [1], all'immagine (artt. 10 c.c. e 96, 97, l. n. 633/1941), alla riservatezza (d.lgs. n. 196/2003, ora adeguato, con d.lgs. n. 101 del

[1] Per effetto dell'abrogazione dell'art. 594 c.p. – disposta dal d.lgs. 15.1.2016, n. 7, attuativo della l. 28.4.2014, n. 67 – l'ingiuria risulta ora sanzionata solo come un illecito civile, la cui commissione comporta per il responsabile sia l'obbligo di risarcire il danno secondo le leggi civili, sia il pagamento di una sanzione pecuniaria civile a favore dello Stato.

10.8.2018[2], alle disposizioni del Regolamento UE 2016/679[3)][4], al nome (artt. 6 c.c. e 22 Cost.) e all'identità personale, vengono generalmente considerati come diritti qualificanti la personalità morale del soggetto.

È fin troppo noto come una delle problematiche più delicate in materia riguardi l'identificazione della linea di confine tra i diversi diritti che mirano alla tutela della sfera morale del soggetto e il diritto di manifestare liberamente il proprio pensiero, a sua volta costituzionalmente tutelato (art. 21 Cost.). Ovviamente, tale questione ha assunto una connotazione peculiare soprattutto per effetto della diffusione dei mezzi di comunicazione di massa e, in particolare, degli strumenti informatici, che ha reso più impellente il bisogno di stabilire i criteri per un equo bilanciamento dei diritti della personalità – e, in particolare, del diritto alla riservatezza – con quelli di cronaca e di critica.

Oltremodo complessa si presenta, in particolare, la problematica, sulla quale si tornerà in seguito, relativa alla identificazione dei limiti riguardanti la possibilità di chiedere che le notizie attinenti a vicende personali siano rimosse dal web. Si tratta, in proposito, di stabilire i confini entro cui è destinato a spaziare il c.d. diritto all'oblio, il quale rappresenta un nuovo profilo del diritto alla riservatez-

---

[2] Tale decreto, pubblicato sulla G.U. il 4 settembre 2018, è entrato in vigore il successivo 19 settembre.

[3] Noto con l'acronimo GDPR (*General Data Protection Regulation*), tale Regolamento, su cui si tornerà ampiamente più avanti, presenta un approccio più moderno all'istituto del consenso informato, prevedendo forme di manifestazione della volontà maggiormente libere e snelle rispetto a quelle contemplate dal Codice della Privacy (d.lgs. n. 196/2003). Ciononostante, il GDPR riserva ai dati personali una protezione, almeno sotto alcuni aspetti, sicuramente più incisiva, introducendo il diritto alla revoca, la presunzione di inefficacia e obblighi più rigidi di informazione.

Comunque, in senso critico nei confronti della rilevanza attribuita dal Regolamento al consenso dell'individuo – considerato in generale strumento non pienamente idoneo a tutelare i soggetti delle cui informazioni si tratta – v. I.A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione,* in *Diritto Mercato Tecnologia*, 2017, 67 ss., la quale manifesta, al riguardo, il dubbio che "l'informazione prestata non sia in grado di influire sulla consapevolezza dell'atto di volontà del singolo". Per gli interrogativi che, in materia, suscitano le tecnologie più recenti, cfr. A. Mantelero, *The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics,* in *Computer Law and Security Review*, 2014, 643 ss.

[4] Il diritto alla riservatezza, che qui più immediatamente interessa, si configura, secondo la ricostruzione corrente, come il diritto del soggetto, indipendentemente dalla sua notorietà (Cass. 27.5.1975, n. 2129, in *Riv. dir. internaz.* 1980, 293, e Cass. 25.3.2003, n. 4366, in *Giust. civ.* 2004, I, 2417), ad evitare ingerenze nella intimità della propria sfera privata, il quale trova il suo referente normativo, nel contesto del principio generale dell'art. 2 Cost., oltreché nel d.lgs. n. 196/2003 (che, lo si ripete, è stato adeguato, col d.lgs. n. 101/2018, al GDPR n. 679/2016), già nelle disposizioni di cui agli artt. 6 e 10 c.c., negli artt. 614, 615 *bis* e 616 c.p. e, a livello sopranazionale, nell'art. 8 della Convenzione europea dei diritti dell'uomo e nell'art. 7 della Carta dei diritti fondamentali dell'Unione Europea.

za [5] ed è stato espressamente riconosciuto dall'art. 17 del Regolamento U.E. n. 2016/679.

Pare quasi inutile sottolineare come tanto il diritto alla riservatezza, quanto il diritto all'oblio risultino inevitabilmente destinati ad assumere una portata più ampia e a sollevare questioni maggiormente delicate quando gli stessi, collocati all'interno dello spazio digitale, siano riferiti alla persona minore di età, su cui pure è specificamente intervenuto il Regolamento U.E., seguito dal d.lgs. n. 101/2018.

2. La disciplina dell'accesso ai servizi della società dell'informazione da parte dei minori

Il Regolamento U.E n. 2016/679, entrato in vigore il 25 maggio 2018 [6], relativamente all'utilizzo di sistemi digitali, nell'occuparsi specificamente della capacità del minore di prestare il consenso (colmando, così, una lacuna presente nella precedente normativa), ha previsto, al paragrafo 1 dell'art. 8 ("Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione"), che, "per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni" [7]. Nel paragrafo 2 si legge, poi, che "il titolare del trattamento si adopera in

[5] Così, già Cass. 9.4.1998, n. 3679, in *Foro it.,* 1998, I, 1834. Nel medesimo senso si è orientata, di recente, Cass., sez. un., 22.7.2019, n. 19681, in *Giust. civ. mass.,* 2019, su cui si tornerà più avanti.

[6] L'articolato è significativamente preceduto da diversi Considerando, tra i quali rilevano, per quanto concerne la posizione del minore, i punti 38 e 58. Il primo statuisce che "i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore" (ad esempio, servizi a tutela dei minori in caso di cyberbullismo o altri servizi per l'infanzia, come telefono azzurro). Nella parte finale del Considerando 58 si legge, poi, che "dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente".

[7] Secondo G. Spoto, *Disciplina del consenso e tutela del minore,* in S. Sica, V. D'Antonio,

ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili"[8]. Infine, il paragrafo 3 dispone che "il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore"[9].

È da sottolineare come il d.lgs. n. 101/2018 abbia utilizzato lo spazio di manovra concessogli dalla normativa sopranazionale riducendo a 14 anni l'età minima per esprimere il consenso al trattamento dei propri dati. In effetti, il d.lgs. n. 196/2003 non prevedeva in via generale nulla in ordine alla capacità del minore di prestare un valido consenso. Il comma 1 dell'art. 2-*quinquies* del novellato Codice Privacy, così come modificato, appunto, per effetto del d.lgs. n.

G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Cedam, 2016, 125, meglio sarebbe stato se il GDPR, piuttosto che indicare un'età prefissata per il consenso, avesse valorizzato la effettiva maturità psicofisica del minore quale concreto elemento di discrimine. A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo,* in *Nuove leggi civ. comm*., 2017, 419, dal canto suo, osserva come nel nostro ordinamento sia destinato a rimanere "senza soluzione l'interrogativo se il minore, capace di discernimento, sia legittimato a prestare personalmente il consenso e se, di fronte a delle violazioni, possa adire l'Autorità Garante per l'attivazione dei rimedi inibitori". Al riguardo, non si può fare a meno di considerare come in Italia, secondo quanto si è già registrato in altri ordinamenti e, anche in applicazione di principi affermati a livello sopranazionale, risulti essere, sia pure solo di recente, ampiamente valorizzata la concreta capacità di discernimento del minore (sul punto v. *infra*, par. 5). In proposito, v. quanto osservato in E. Quadri, in F. Bocchini ed E. Quadri, *Diritto privato*, Giappichelli, 2018, spec. 274. Per un approfondimento del concetto di ''capacita' di discernimento'', v., comunque, E. La Rosa, *Tutela dei minori e contesti familiari,* Giuffrè, 2005, 69 ss., la quale descrive significativamente la stessa come "lo strumento per la concretizzazione del valore della differenza, dal momento che rende operativo un trattamento giuridico commisurato al reale processo evolutivo del minore, equiparandolo all'adulto, allorché abbia raggiunto maturità di giudizio e assoggettandolo alla disciplina dell'incapacità, se non sia in possesso del discernimento necessario per adottare scelte autonome e coscienti". V., inoltre, M. Piccinni*, I minori di età*, in C.M. Mazzoni e M. Piccinni, *La persona fisica,* nel *Trattato Iudica Zatti*, Giuffrè`, 2016, 407 ss., e G. Recinto e F. Dell'Aversana, *I rapporti personali del minore*, in F. Rossi (a cura di), *Capacità e incapacità*, Esi, 2018, 44 ss.

[8] C. Perlingieri, *La tutela dei minori di età nei social networks,* in *Rass. dir. civ.*, 2016, 1332, osserva, in proposito, come "soltanto mediante la conoscenza dell'operatività dei criteri degli algoritmi che regolano il flusso dei contenuti" sia possibile consentire "ai genitori scelte consapevoli in ordine alla manifestazione di consenso all'iscrizione dei figli al *social network*, nonché alla costante verifica della idoneità della piattaforma allo sviluppo del minore".

[9] Dal paragrafo 3 dell'art. 8 sembrerebbe doversi ricavare che se il minore ha raggiunto l'età per un valido consenso al trattamento dei dati, ma non quella per poter concludere validamente il contratto, quest'ultimo sarà invalido e il trattamento dovrà cessare (così, F. Naddeo, *Il consenso al trattamento dei dati personali del minore,* in *Dir. dell'informazione e dell'informatica,* 2018, 27 ss.). Sulla "scissione tra consenso contrattuale e consenso privacy", v., inoltre, I.A. Caggiano, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione, in www.rivistafamilia.it,* 2018*, passim.*

101/2018, dispone, invece, che "in attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale".

La ragione dell'attenzione che prima il legislatore europeo e poi quello nazionale hanno inteso riservare alla questione concernente le condizioni per l'accesso ai servizi della società dell'informazione da parte dei minori trova, evidentemente, giustificazione nella progressiva, esponenziale diffusione dell'uso di Internet e nella tendenziale libertà di connettersi e, conseguentemente, di accedere ai servizi online: ciò per chiunque e, quindi, anche per chi non abbia ancora compiuto la maggiore età.

Accanto al tradizionale personal computer, esistono, in effetti, ormai, diversi altri dispositivi mobili (dai tablet, ai notebook, agli smartphone, ai palmari), in quanto tali senz'altro agevolmente disponibili anche da parte dei più giovani. La possibilità di accedere ad Internet e ai diversi servizi offerti dalla rete risulta, quindi, almeno potenzialmente, per chiunque, appunto, del tutto illimitata. E, così, i ragazzi, ma perfino i bambini, si imbattono con frequenza nelle pubblicità di venditori che offrono servizi per loro particolarmente allettanti, dagli abbonamenti per scaricare la musica preferita, ai videogiochi, ai film.

L'evoluzione tecnologica, penetrata oramai profondamente nella realtà sociale, se da un lato presenta, allora, indiscutibili, significativi vantaggi, dall'altro è inevitabilmente destinata a suscitare serie perplessità in ordine ai rischi connessi ad un uso potenzialmente indiscriminato, da parte dei minori, degli strumenti attraverso cui la stessa si esprime.

Si tratta, evidentemente, di un fenomeno destinato a determinare il nascere di problematiche concernenti non solo delicati aspetti sociali, culturali e psicologici, ma anche significativi profili di tipo giuridico, finendo col risultare coinvolti e suscettibili di essere compromessi i diritti fondamentali e costituzionalmente protetti dei minori [10].

Negli ultimi anni si è, inoltre, registrato un notevole incremento dell'uso dei social network da parte dei minori: ormai non esiste, in effetti, un solo adolescente (ma il discorso può estendersi senz'altro anche ai bambini di otto/dieci anni) che non conosca reti sociali come Facebook, Instagram, Twitter, Snapchat, WhatsApp, YouTube.

[10] E. Andreola, *Minori e incapaci in* Internet, Esi, 2019, 12, definisce il minore come "il consumatore più debole tra i consumatori", poiché "mentre il consumatore è occasionalmente il soggetto debole del contratto, il minore lo è per *status*".

I social network consentono una circolazione dei dati estremamente rapida e favoriscono la condivisione di ogni genere di informazione (fotografie, video, registrazioni vocali, opinioni, ecc.) con un numero elevatissimo di utenti, senza alcun limite geografico [11].

È chiaro, allora, che, ove ad accedere ad Internet sia un minore, presumibilmente non dotato di un livello di maturità tale da consentirgli di utilizzare le nuove forme di comunicazione in rete con la dovuta cautela, le possibilità che si verifichino abusi ai suoi danni risultano – come le cronache, del resto, non mancano continuamente di palesare – senz'altro esponenzialmente più elevate [12].

La scelta di introdurre dei meccanismi atti a proteggere i minori, in quanto soggetti senz'altro maggiormente vulnerabili, dai rischi connessi all'uso spesso indiscriminato della rete Internet si è rivelata, di conseguenza, anche da noi progressivamente sempre più improcrastinabile, soprattutto in considerazione del fatto che negli Stati Uniti la disciplina del trattamento online dei dati personali

[11] Sul punto, v. le osservazioni di E. Andreola, *Minori*, cit., 94, secondo la quale "deve essere riconosciuto al minore il diritto all'informazione sul *web*", essendo detta prerogativa riconducibile a quanto disposto dall'art. 13, comma 1, della Convenzione Onu sui diritti dell'infanzia e dell'adolescenza, che sancisce il diritto del minore alla libertà di espressione, da intendersi come "libertà di ricercare, di ricevere o di divulgare informazioni ed idee di ogni specie, indipendentemente dalla frontiere, sotto forma orale, scritta, stampata o artistica, o con ogni altro mezzo a scelta del fanciullo". Analogamente, aggiunge l'a., deve essere riconosciuto al minore "il diritto di aderire a *social network* e *community,* quali forme di aggregazione e associazione *online*". "Il divieto di accesso ai *social media*", osserva, quindi, l'a., "comporterebbe per il minore, nell'era digitale, un limite ingiustificato alla partecipazione scolastica, civile, culturale e associativa".

[12] E il problema riguarda, ovviamente, sia il minore "vittima" dell'eventuale illecito commesso attraverso il web, sia il minore "artefice" di tale illecito, con la connessa problematica della responsabilità dei genitori, i cui principi devono ormai sempre più frequentemente confrontarsi, appunto, con le potenzialità dannose che si riconnettono all'uso delle tecnologie qui in discussione. Al riguardo, v. la significativa pronuncia del Tribunale di Teramo (sent. n. 18 del 16.1.2012, in *DeJure*), il quale ha affermato che "ai fini dell'esonero dalla loro responsabilità" i genitori devono fornire "la prova liberatoria di non aver potuto impedire il fatto, il che, nel caso di illecito commesso attraverso "social network" (nel caso di specie "Facebook"), si concretizza in una limitazione per forza di cose quantitativa e qualitativa dell'accesso alla rete internet". Cfr., inoltre, Trib. Caltanissetta, 16.7.2018, in *www.ilFamiliarista.it*. Sul punto, v., peraltro, le recenti osservazioni di E. Andreola, *Minori*, cit., 16, secondo la quale non si può in ogni caso fare a meno di considerare la "peculiarità del mezzo di comunicazione", che sembra "dover incidere sul contenuto dell'obbligo di vigilanza e sulla reale possibilità o esigibilità del controllo parentale (ai fini dell'esimente di cui all'art. 2048 c.c.)". "Infatti", precisa l'a., "se è vero che il genitore consapevole dei pericoli della navigazione cibernetica, ove acconsenta all'accesso in rete del figlio, ne è responsabile, è altrettanto vero che, per sua stessa natura, lo strumento informatico (*computer*, *tablet* e, ancor di più, *smartphone*) si presta a un impiego individuale e lontano da occhi indiscreti. Inoltre, il riconoscimento della *privacy* del minore impone un contemperamento tra obbligo di vigilanza e autonomia dei minori, anche nei casi particolari del genitore lontano, separato, divorziato o adottivo".

dei minori risale ad oltre venti anni fa [13]. E, al riguardo, pare il caso di osservare come tutte le principali piattaforme online, quali Facebook, Instagram, WhatsApp, Snapchat e YouTube, essendo, appunto, nordamericane, rispettino il più basso limite dei 13 anni, quale previsto dalla normativa vigente negli Stati Uniti circa il trattamento dei dati personali dei minori [14].

3. I dubbi relativi alla idoneità del meccanismo introdotto dal GDPR 2016/679 (e recepito dal D.lgs. n. 101/2018) a tutelare i diritti dei minori nello spazio digitale

Il problema, allora, una volta finalmente introdotta una normativa della cui necessità certo non pare sia possibile dubitare, si sposta su un altro piano, trattandosi di valutare la reale idoneità del meccanismo introdotto dal GDPR 2016/679, e recepito dal d.lgs. n. 101/2018, ad offrire una concreta efficace tutela del diritto alla protezione dei dati dei minori che si muovono all'interno dello spazio digitale [15], dove, sembra il caso di insistere sul punto, le insidie ed i rischi [16] finiscono con l'aumentare esponenzialmente, a causa dell'ampia

[13] Ci si riferisce al *Children's Online Privacy Protection Act (COPPA)* del 1998, poi modificato nel 2013, che fissa a 13 anni il limite al di sotto del quale non è possibile prestare il consenso al trattamento dei dati personali e che stabilisce che coloro i quali offrono servizi ai minori, raccogliendone, quindi, i dati, devono informare i genitori ed ottenere il loro *verifiable consent*. Per un'analitica disamina della disciplina statunitense in materia, si rinvia a M. Diffenderfer, *The righys of privacy and publicty for minors online: protecting the privilege of disaffirmace in the digital,* in *U. Lousville Law Review*, 2016, 131.

[14] F. Naddeo, *op. cit.,* 27 ss. – riportando i risultati di uno studio già pubblicati da M. Diffenderfer, *op. cit*., 131 – ricorda che "da una ricerca condotta negli Stati Uniti negli ultimi anni risulta che circa il 95% dei minori, dai dodici ai diciassette anni, navigano online; di questi, il 75% lo fa quotidianamente e circa il 50% più volte al giorno. Degli adolescenti intervistati, l'80% utilizza i siti di social network. La ricerca mostra anche che gli adolescenti condividono maggiori quantità di informazioni personali su se stessi sui siti di social media rispetto agli anni passati, segnalando aumenti costanti nella frequenza con cui essi pubblicano immagini di se stessi e forniscono nomi di scuole, città di residenza, indirizzi email e numeri di cellulare".

[15] *E* resta comunque aperta anche l'ulteriore problematica che concerne, più in generale, l'idoneità – nell'ambiente digitale – dello strumento del consenso a tutelare sufficientemente la persona, quindi anche adulta, dei cui dati si tratta. Per i dubbi riguardo all'efficacia del consenso ai fini della protezione dei dati contro i rischi per le libertà dell'individuo, v. le considerazioni svolte, di recente, in L. Gatt, R. Montanari e I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali,* in *Politica del diritto,* 2017, 339 ss. V., inoltre, più specificamente in relazione alla situazione del minore, I.A. Caggiano, *Privacy e minori*, cit., *passim*.

[16] Basti pensare alla pedopornografia, al *cyberbullismo*, nonché ai recenti fenomeni della *blue whale,* del *blackout* e del *revenge porn.*

condivisione di dati, spesso anche sensibili.

Ai sensi dell'art. 8 del GDPR, come anticipato, "ove il minore abbia un'età inferiore ai 16 anni" il trattamento dei suoi dati personali "è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale".

Ebbene, se da un lato non può che condividersi la bontà dell'intenzione che ha indotto il legislatore ad una tale soluzione, dall'altro non si può fare a meno di rilevare il rischio che la previsione dell'intervento del titolare della responsabilità genitoriale venga, pure piuttosto agevolmente, aggirata con la creazione, da parte del minore, di profili falsi [17], tanto più che lo stesso legislatore ha ritenuto, forse fin troppo fiduciosamente, di rimettere al titolare del trattamento e alla sua responsabilità il comunque difficile compito di individuare i criteri più idonei ad identificare il titolare della responsabilità genitoriale.

In effetti, al fine di predisporre un meccanismo concretamente idoneo a tutelare i minori contro i rischi connessi all'uso del web, sarebbe stato probabilmente più opportuno che il legislatore europeo, sulla falsariga di quanto stabilito negli Stati Uniti, avesse introdotto un sistema di controllo maggiormente mirato e destinato alla inequivocabile identificazione dei genitori chiamati ad intervenire [18].

Resta aperta, d'altro canto, la problematica identificazione del soggetto legittimato a prestare o autorizzare il consenso, poiché l'art. 8 si limita a richiedere l'intervento del "titolare della responsabilità genitoriale", senza precisare se sia sufficiente il consenso di uno solo dei due genitori o se invece sia necessario quello di entrambi gli esercenti la responsabilità. E il problema, ovviamente, è destinato ad emergere soprattutto allorché si tratti di coppie separate o divorziate, evidentemente nella prospettiva della distribuzione del potere decisionale tra i genitori (ai sensi degli artt. 337 ter e 337 quater c.c.).

Ancora, resta da definire se tale espressione debba essere interpretata estensivamente, in modo da ricomprendere – come sembra, invero, quasi inevitabile – qualsiasi persona che eserciti la responsabilità di genitore su un minore (*ex* art. 2 n. 8 del Regolamento di Bruxelles II *bis*) [19], compreso, quindi, eventualmente, il tutore [20].

---

[17] A. Thiene*, op. cit*., 420, riporta, al riguardo, uno studio condotto da G. Mascheroni e K. Òlafsson*,* Net children go mobile*: il report italiano*, Osscom, Università Cattolica del Sacro Cuore, Milano, 2015, 16 ss., secondo il quale, la maggior parte dei ragazzi tra i 9 e i 12 anni ha indicato sul proprio profilo Facebook, che impone il limite di età dei 13 anni, un'età non corretta.

[18] V. *infra*, nota 69.

[19] Il 24 maggio 2019 è stata approvata in via definitiva la revisione di tale Regolamento, la quale si applicherà a partire da tre anni dopo la sua pubblicazione nella Gazzetta Ufficiale dell'U.E. Il riformato art. 2, n. 8 precisa che è "titolare della responsabilità genitoriale" la persona, istituzione o altro ente che eserciti la responsabilità di genitore su un minore.

[20] In tal senso, G. Spoto, *op. cit.*, 115.

Riguardo all'accennata situazione di crisi familiare, deve ritenersi che, ove il minore intenda iscriversi a siti o social network, aprire un account di posta elettronica o creare altri account personali, occorra senz'altro il consenso di entrambi i genitori esercenti la responsabilità genitoriale [21], almeno se le parti non abbiano optato per l'esercizio disgiunto della responsabilità per le decisioni di ordinaria amministrazione [22].

Nell'ipotesi, poi, in cui le parti, al riguardo, abbiano scelto di comune accordo di esercitare disgiuntamente la responsabilità genitoriale, diventa, ovviamente, indispensabile identificare preliminarmente la natura dell'atto che si intenda compiere, al fine di comprendere se si tratti di atto di ordinaria amministrazione o di una delle "decisioni di maggiore interesse per i figli" e, quindi, se sia sufficiente il consenso di uno solo dei genitori o se occorra comunque quello di entrambi.

In proposito, considerata la qualificazione in termini di diritto fondamentale del diritto alla protezione dei dati personali, secondo quanto risulta del resto confermato dall'art. 1 del GDPR, pare invero non si possa fare a meno di considerare, in linea di principio, quella relativa al trattamento dei dati del figlio minore una iniziativa rientrante tra le decisioni di maggiore interesse per lo stesso, in quanto tale adottabile solo previo consenso di entrambi i genitori [23].

---

[21] In proposito, pare il caso di ricordare come, ai sensi dell'art. 337 *ter*, co. 3, c.c., in caso di disaccordo la decisione sia rimessa al giudice.

[22] Così, tra gli altri, A. Simeone, *Tutela della privacy dei minori rafforzata con il GDPR: chi apre l'account Facebook dell'infrasedicenne figlio dei genitori separati?* in *www.ilFamiliarista.it,* 25.5.2018. Sul punto, v., per la giurisprudenza, l'orientamento di Trib. Mantova, 19.9.2017, in *www.Ilfamiliarista.it*, 18.1.2018, con nota di S. Molfino, *Vietato pubblicare le foto dei figli sui social network senza il consenso dell'altro genitore, passim*.

[23] V. quanto osservato al riguardo da S. Molfino, *Il diritto d'immagine del minore in rete: profili di responsabilità genitoriale e ipotesi di risarcimento del danno,* in *www.Ilfamiliarista.it,* 9 gennaio 2017, 3 ss., secondo il quale, ove si tratti di "concedere ad una società una licenza non esclusiva e trasferibile a terzi per l'utilizzo dell'immagine di un soggetto minore", siamo in presenza di atti che necessitano "quantomeno della decisione congiunta dei genitori esercenti la responsabilità genitoriale". Il riferimento dell'autore è alla questione, affrontata dal Tribunale di Roma il 1°.6.2015 (in *Redazione Giuffrè,* 2015), riguardante il rapporto contrattuale tra utente e social network (nella specie Facebook): nel caso di pubblicazione di immagini su Facebook – osserva il Tribunale – non vengono ceduti integralmente i diritti fotografici, ma viene ceduta la sola licenza non esclusiva, trasferibile, per l'utilizzo di qualsiasi contenuto IP (ossia il contenuto coperto da diritti di proprietà intellettuale, come foto e video) pubblicato sul social network. Del resto, per il necessario consenso di entrambi i genitori si sono orientati, già prima della entrata in vigore del GDPR, sia il Tribunale di Roma (provvedimento del 23.12.2017, in *Resp. civ. e prev.*, 2018, 589 ss., con nota di S. Peron, *Sul divieto di diffusione sui social network delle fotografie e di altri dati personali dei figli,* in *Resp. civ. e prev*., 2018, 589 ss.), sia il Tribunale di Mantova (provvedimento del 19.9.2017, cit.). In proposito, particolarmente significativa sembra una recente pronuncia del Tribunale di Rieti (6.3.2019, in *www.ilFamiliarista.it,* 25 marzo 2019), il quale,

Riguardo alla scelta del legislatore europeo di non fare alcun riferimento all'ipotesi in questione, sembra, allora, il caso di osservare come, se è vero che l'esercizio della responsabilità genitoriale è regolamentato diversamente nei differenti paesi europei, con la conseguente difficoltà di individuare una disciplina unitaria del consenso al trattamento dei dati del minore (figlio di genitori separati o divorziati), tutt'altro che infondato risulti il timore che – in mancanza di una regolamentazione, al riguardo, di un fenomeno in esponenziale crescita, quale quello dell'uso di Internet e dei social network da parte dei minori, in un contesto sociale notoriamente caratterizzato dalla sempre maggiore tendenza alla rottura della comunità di vita tra i genitori – possa finire con l'acuirsi la conflittualità all'interno di quelle coppie in cui, sia pure – come pare, peraltro, inevitabile – solo strumentalmente, le parti manifestino divergenti opinioni riguardo alla scelta di pubblicare su Internet le immagini dei figli [24].

Ulteriore, delicata questione è quella che concerne la validità del consenso al trattamento nel caso in cui il minore abbia occultato la propria età. Non pare che, in una evenienza del genere, possa ritenersi senz'altro applicabile la generale disposizione di cui all'art. 1426 c.c., secondo il quale il contratto concluso da un minore non è annullabile allorché lo stesso abbia "con raggiri occultato la sua minore età" (fermo restando che "la semplice dichiarazione da lui fatta di essere maggiorenne non è di ostacolo all'impugnazione del contratto") [25]. Dalla lettura

---

su istanza di una donna divorziata che lamentava la pubblicazione sui social network di immagini dei propri figli da parte della compagna del marito – richiamando sia il GDPR 679/2016, sia il recente d.lgs. n. 101 del 2018, nonché le due ricordate pronunce dei Tribunali di Mantova e Roma – ha concluso che "ritenuta la domanda sorretta dai requisiti del *fumus boni iuris* e *del periculum in mora*", ricorrono anche i presupposti dello strumento cautelare e, quindi, "il ricorso deve essere accolto, con conseguente condanna della resistente alla rimozione – dai propri profili social – delle immagini relative ai minori…ed alla contestuale inibitoria dalla futura diffusione di tali immagini, in assenza del consenso di entrambi i genitori".

In proposito, v. le considerazioni svolte da C. Perlingieri, *La tutela dei minori,* cit., 1337 ss., secondo la quale il contratto dell'utente minore con la piattaforma sociale "può essere validamente concluso soltanto con il consenso dei soggetti esercenti la responsabilità genitoriale".

[24] Sul punto, v. A. Simeone, *op. cit.*

[25] Sulla natura del contratto concluso tra il sito di social network e l'utente, v. C. Perlingieri, *Gli accordi tra i siti di social networks e gli utenti,* in *Rass. dir. civ*., 2015, 115, la quale, nel ricondurre lo stesso nell'ambito dei contratti di scambio, osserva come "la disposizione della *privacy* e dei dati personali" sia stabilita "in funzione dell'utilizzo della piattaforma, sì che in virtù del sinallagma, l'utente in tanto ha il diritto di utilizzare la piattaforma – e il *social* è obbligato a consentirne l'utilizzo – in quanto il *social* può raccogliere e sfruttare i dati personali. Tale conclusione induce a dubitare seriamente dell'affermazione secondo la quale il *social network* non è obbligato a fornire il servizio, né deve assicurare il corretto funzionamento della piattaforma, dal momento che queste prestazioni costituiscono il corrispettivo della licenza concessa dall'utente". Sul punto, v., più di recente, G. Resta, *Diritti fondamentali e diritto privato nel contesto digitale*, in F. Caggia e G. Resta (a cura di), *I diritti fondamentali in Europa e il diritto privato*, Roma Tre-Press,

dell'art. 8 GDPR sembrerebbe, infatti, che il trattamento sia destinato a restare valido anche in mancanza di raggiri da parte del minore, purché il titolare del trattamento abbia agito nel rispetto della previsione di cui al paragrafo 2 dell'art. 8.

Infine, resta la dubbia interpretazione circa l'effettiva portata di quanto disposto dal Considerando 71, per il quale le profilazioni non dovrebbero comunque riguardare il minore.

In effetti, come chiarito dal *Working Party Art. 29* nelle linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679, aggiornate al 6 febbraio 2018, il fatto che il divieto sia collocato in un Considerando non potrebbe portare senz'altro ad escludere che ai minori possano applicarsi profilazioni e decisioni automatizzate. Residuerebbero, dunque, anche per i minori tutte (e solo) le eccezioni (la necessità di concludere un contratto, la previsione autorizzatoria di una norma nazionale o UE e il consenso espresso) che legittimano decisioni automatizzate e profilazioni, di cui all'art. 22 del GDPR, che non fa alcuna distinzione tra gli adulti e i minori.

Ma, invero, lo stesso consenso del minore non sembra costituire strumento sufficiente a tutelare quest'ultimo di fronte a decisioni basate su informazioni ricavate dall'incrocio di dati prelevati da varie forti online e processate da algoritmi [26].

Le linee guida, che pure in alcuni passaggi risulta abbiano preso in considerazione la necessità di offrire ai minori una garanzia di tutela più radicale, non sembrano, peraltro, portare alle logiche conseguenze le premesse da cui partono. Nelle stesse si legge, infatti, che, rappresentando i minori un gruppo molto vulnerabile, le imprese dovrebbero astenersi dal profilarli per scopi di marketing. Nei giochi online, si legge ancora nelle linee guida, la profilazione [27] può servire

---

2019, 128 ss., il quale, in particolare, si chiede "se i dati personali possano costituire una valida controprestazione – e segnatamente la principale controprestazione – di un contratto di fornitura di contenuti digitali". L'a. ricorda, al riguardo, come l'Autorità antitrust italiana abbia ritenuto il Codice del consumo applicabile alla fattispecie di fornitura di servizi della società dell'informazione a titolo formalmente 'gratuito', in quanto il valore economico dei dati personali era tale da giustificare la sussistenza di un rapporto di scambio a carattere sostanzialmente sinallagmatico (cfr. AGCM, 11.5.2017, n. 26597, WhatsApp-Trasferimento Dati a Facebook, in Bollettino n. 18/2017, 57, nonché AGCM, 11.5.2017, n. 26596, WhatsApp-Clausole Vessatorie, in Bollettino n. 18/2017). L'a. mette in luce come, in ogni caso, dalle disposizioni di cui agli artt. 4, n. 10 e 7, comma 4 del GDPR non emerga l'impossibilità di dare vita ad una relazione sinallagmatica tra la prestazione di un servizio e la messa a disposizione di dati e metadati.

[26] Sulle modalità attraverso cui avviene la memorizzazione automatica e la conservazione delle informazioni che immettiamo nella rete quando navighiamo, v. l'attenta analisi di F. Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di internet,* in G. Comandè (a cura di)*, Persona e tutele giuridiche*, Torino, 2003, *passim*.

[27] Sui "trattamenti occulti" e la profilazione degli utenti, v. l'analisi operata da A. Mantelero,

per individuare i giocatori che l'algoritmo ritiene più propensi a spendere soldi e a fornire annunci pubblicitari più personalizzati: l'età e la maturità del minore possono influenzarne la capacità di comprendere la motivazione che sta alla base di tale tipo di marketing o le sue conseguenze. Nonostante tali sicuramente condivisibili considerazioni, le medesime linee guida si limitano a concludere che la soluzione normativa più adatta sia quella dei codici di condotta, ossia la *self regulation*. Ma – al di là dei dubbi riguardanti la reale idoneità di tali codici a consentire ai minori un'agevole identificazione dei contenuti commerciali e dell'intento persuasivo dei messaggi online – la relativa adozione, come si evince dalla disposizione di cui all'art. 40, paragrafo 2, del GDPR, si presenta meramente facoltativa, con la conseguenza che in caso di mancata adozione degli stessi, non sarebbe possibile attivare alcuna azione nei riguardi del responsabile del trattamento per violazione delle regole di condotta [28].

4. Il diritto all'oblio

Dall'art. 17 del GDPR [29], alla luce dei Considerando 65 e 66 [30] del medesimo

Attività di impresa in Internet e tutela della persona, Cedam, 2004, 146 ss. V., inoltre, G. Ramaccioni, *La protezione dei dati personali e il danno non patrimoniale*, Jovene, 2017, 242 ss., nonché, più di recente, G. De Gregorio e R. Torino, *Privacy, protezione dei dati personali e* big data, in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Lefebvre, 2019, 478 ss.

[28] Per un approfondimento delle principali novità relative ai codici di condotta di cui all'art. 40 del GDPR, v. D. Poletti e M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), *Privacy Digitale*, cit., 369 ss. Le aa. si soffermano, inoltre, sulle nuove *"Regole Deontologiche"* di cui all'art. 2-*quater* del GDPR, cui ha fatto seguito la pubblicazione, nella Gazzetta Ufficiale n. 3 del 4 gennaio 2019, della delibera del Garante per la protezione dei dati personali del 29 novembre 2018, recante «Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica pubblicate ai sensi dell'articolo 20, comma 4, del decreto legislativo 10 agosto 2018, n. 101».

[29] I cui paragrafi 1 e 2 recitano testualmente: "1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

Regolamento, si ricava che, nel caso in cui il consenso sia stato prestato dai genitori esercenti la responsabilità in nome e per conto del minore infrasedicenne, quest'ultimo, al compimento del sedicesimo anno di età, può sia acconsentire personalmente al trattamento dei dati, sia chiedere al titolare la cancellazione senza ingiustificato ritardo [31].

Più specificamente, ai sensi del paragrafo 1, lettera f) dell'art. 17, l'interessato ha il diritto di ottenere la cancellazione dei dati quando gli stessi "sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1".

Secondo la giurisprudenza che si è occupata fin qui del diritto all'oblio, con riguardo, cioè, alla diffusione delle pubblicazioni su carta, tale diritto – qualificato come "un nuovo profilo del diritto alla riservatezza" [32] – doveva essere in-

---

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

In senso critico nei confronti della "oscura formulazione" di tale disposizione, v. F. Di Ciommo, *Il diritto all'oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali,* in *Foro it.*, 2017, V, 306 ss.

[30] Nel Considerando 65 del GDPR si legge, con specifico riferimento alla problematica qui in esame, che il diritto all'oblio "è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore".

Nel Considerando 66 si legge, poi, che "per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali".

[31] Per i dubbi circa la reale funzionalità della nuova disciplina, v. *infra*, spec. note 47 e 48.

[32] Così, Cass. 9.4.1998, n. 3679, cit., per la quale lo stesso si configura come diritto inviolabile dell'uomo. Più di recente, v. Cass. 20.3.2018, n. 6919, in *Giust. civ. mass.,* 2018, in cui si parla senz'altro di "diritto fondamentale all'oblio". V., inoltre, Cass., sez. un., 22.7.2019, cit. *supra*, nota 5. Per dubbi circa la configurabilità del diritto all'oblio quale nuova voce dei diritti della personalità, v., peraltro, G. Finocchiaro*, Il diritto all'oblio nel quadro dei diritti della personalità*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google-Spain,* 29 ss.

teso quale "legittimo interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata". Il diritto all'oblio finiva col gravitare, dunque, attorno a due punti fermi concettuali: il tempo e l'utilità sociale della notizia. Il tempo rilevava in quanto era il decorso dello stesso a giustificare la pretesa del soggetto di riappropriarsi di notizie sul proprio conto [33]. Il fattore della utilità sociale della notizia, invece, rilevava in senso negativo, essendo proprio l'inesistenza di una utilità sociale insita nella rievocazione delle notizie a far prevalere il diritto all'oblio sul diritto all'informazione [34].

Tale diritto si presentava, dunque, come una sorta di divieto di "ripubblicazione" di una notizia destinata, insomma, non già ad essere cancellata, bensì a non essere riproposta nel tempo [35].

Pare chiaro, allora, come il "diritto all'oblio", quale ricostruito alla luce di una simile impostazione ermeneutica, non risulti armonizzarsi pienamente col diverso "diritto alla cancellazione" dei dati, in cui l'art. 17 del Regolamento sembra volerlo risolvere [36].

Con la nascita dell'era digitale e la progressiva diffusione di Internet, si è registrata sia una rilevante intensificazione degli interventi giurisprudenziali in materia, sia una diversa tipologia di approccio al tema.

La giurisprudenza che si è occupata in tempi più recenti del diritto all'oblio – nel definire evocativamente la rete Internet, in cui oramai confluiscono tutte le notizie, come "un oceano di memoria" [37] – ha mostrato, infatti, a ragione, di preoccuparsi non più, secondo l'accennata impostazione, dei rischi legati alla eventuale ripubblicazione della notizia, ma di quelli derivanti dalla perpetuazio-

---

[33] Sul punto, v., di recente, Trib. Lucca, 19.1.2019, n. 96, in *Redaz. Giuffrè*, 2019. Secondo il Tribunale toscano, il diritto all'oblio "va escluso qualora tra i fatti da cui la vicenda si origina ed il momento finale della vicenda medesima sia trascorso un intervallo breve, innegabilmente insufficiente ad affievolirne l'interesse collettivo alla conoscenza e divulgazione".

[34] In tal senso, S. Morelli, *Fondamento costituzionale e tecniche di tutela dei diritti della personalità di nuova emersione (a proposito del "diritto all'oblio")*, in *Giust. civ.,* 1997, 515.

[35] Così, D. Barbierato, *Osservazioni sul diritto all'oblio e la sua (mancata) novità del regolamento UE 2016/679, sulla protezione dei dati personali,* in *Resp. civ. e prev.,* 2017, 2100 ss. Sul punto, v., inoltre, S. Bonavita e R. Pardolesi, *Gdpr e diritto alla cancellazione (oblio),* in *Danno e resp*., 2018, 269 ss., nonché M. Tampieri, *Il diritto all'oblio e la tutela dei dati personali,* in *Resp. civ. prev*., 2017, 1010 ss.

[36] Diritto che, in alcuni casi, risulta essere comunque recessivo, in quanto determinati dati, per la funzione svolta, non possono essere cancellati. Sul punto, v. F. Mangano, *Diritto all'oblio,* in *Giur. merito*, 2012, 2621 ss. Per il carattere riduttivo della tutela, v. *infra*, nota 48.

[37] Cass. 5.4.2012, n. 5525, in *Guida al diritto* 2013, dossier 5, 44.

ne, attraverso la permanenza in rete, della notizia stessa [38]. Con i nuovi strumenti di comunicazione online, diventa, infatti, sostanzialmente impossibile ipotizzare una reale scomparsa della notizia originariamente diffusa, la quale finisce con l'essere persistentemente memorizzata in archivi sul web [39]. Ciò con la conseguenza che l'eventuale (mero) divieto di ripubblicazione della notizia risulta, a tutta evidenza, strumento non più sufficientemente idoneo a tutelare il diritto all'oblio del soggetto interessato, il quale può – ove si rifletta sulle dinamiche proprie degli attuali mezzi di informazione – trovare adeguata protezione solo attraverso la contestualizzazione e l'aggiornamento della notizia stessa alla luce delle mutate circostanze [40].

Anche tale nuova – e preferibile – impostazione esegetica del diritto all'oblio finisce, peraltro, col palesare l'inadeguatezza dello strumento previsto dall'art. 17: visto che negli anni più recenti il diritto all'oblio ha assunto una grande rilevanza principalmente per effetto della diffusione delle notizie attraverso il web, dove le stesse restano di fatto per sempre e, quindi, possono essere rinvenute in qualsiasi momento da chiunque, non pare che riconoscere all'interessato il diritto alla cancellazione dei dati sia sufficiente a tutelare effettivamente l'interesse protetto, il quale può invece trovare concreta protezione solo attraverso l'aggiornamento della notizia inizialmente riportata da un sito internet [41].

Secondo una ancora più recente – e indubbiamente attenta ai meccanismi degli strumenti informatici – impostazione della Corte di giustizia Ue, pronunciatasi sul famoso caso *Google Spain* [42], il diritto all'oblio si dovrebbe essen-

---

[38] E v.: Corte Edu 19.10.2017, Fuchsmann c. Germania, in *Danno e resp*., 2018, 149, in cui vengono indicati i criteri in base ai quali stabilire se una notizia sia ancora o meno di apprezzabile interesse per la collettività; Cass. 9.8.2017, n. 19761, in *Foro it.* 2017, I, 2989; Cass. 24.6.2016, n. 13161, in *www.giustiziacivile.com* 2016, 9 dicembre.

[39] Sul punto, v. G. Finocchiaro, *La memoria della rete e il diritto all'oblio,* in *Dir. informatica*, 2010, 391 ss.

[40] I termini della questione sembrano, in effetti, correttamente impostati da Cass. 5.4.2012, n. 5525, cit., secondo cui esiste "un diritto di controllo a tutela della proiezione dinamica dei propri dati e della propria immagine sociale, che può tradursi, anche quando trattasi di notizia vera – e *a fortiori* se di cronaca – nella pretesa alla contestualizzazione e aggiornamento della notizia e, se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione". Per un approfondito esame di tale decisione, v. S. Sica e V. D'Antonio, *La procedura di deindicizzazione,* in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio*, cit., 145 ss.

[41] F. Di Ciommo, *Il diritto all'oblio*, cit., 306 ss. Sul punto, v., inoltre, D. Barbierato, *op. cit*., 2100 ss., secondo cui la cancellazione può essere solo eventuale e solo come estrema *ratio*. La norma di riferimento è, invece, il precedente articolo 16, che regola il diritto di rettifica e di integrazione dei dati. Non a caso – precisa l'a. – il dettato normativo dell'articolo 16 riporta lo stesso riferimento temporale ("senza ingiustificato ritardo"), già presente nell'articolo 17.

[42] Corte giust. U.E. 13.5.2014, causa C-131/12, in *Dir. inf*., 2014, 353 ss., nonché in *Foro it*., 2014, IV, 295.

zialmente configurare come diritto alla "deindicizzazione" dei propri dati personali. Per la Corte, l'attività del motore di ricerca, che consiste nel trovare informazioni pubblicate da altri su Internet, nell'indicizzarle in modo automatico e nel memorizzarle temporaneamente, si traduce in un vero e proprio trattamento dei dati personali, per cui "le azioni volte a chiedere la rimozione, cancellazione o deindicizzazione di un contenuto presente su internet, possono essere rivolte sia a chi pubblica le informazioni sia ai gestori dei motori di ricerca". "Il gestore di un motore di ricerca" – continua la Corte – "è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita".

Il gestore, quindi, dovrebbe cancellare dall'elenco dei risultati, a partire dal nome di una persona, tutti i link relativi a pagine web di terzi, riguardanti informazioni relative al soggetto, ove il trattamento non sia più conforme [43]. E la conformità va valutata alla luce del tempo trascorso e dell'effetto indotto dalla indicizzazione sulla fruibilità dei dati.

Così interpretato, il diritto all'oblio sembrerebbe più agevolmente collocabile nella prospettiva propria della disposizione di cui all'art. 17 del Regolamento, ma non si può fare a meno di rilevare come tale ultima previsione nulla dica riguardo alla deindicizzazione di contenuti in Internet e, quindi, i dubbi circa l'applicabilità dell'art. 17 anche ai motori di ricerca sembrano destinati a perpetuarsi.

In ogni caso, al di là delle perplessità in ordine alla ricostruzione della nozione di diritto all'oblio, resta la questione che concerne l'individuazione dei criteri per operare un equilibrato bilanciamento tra tale diritto e il diritto di cronaca.

La Suprema Corte – sul presupposto che il legislatore comunitario non ha precisato in quali casi debba prevalere l'uno o l'altro – con ordinanza n. 28084 del 2018 [44], invocando la fissazione di criteri univoci di bilanciamento, appunto,

[43] La Corte, a ben vedere, non riconosce un diritto assoluto all'oblio, poiché la cancellazione riguarda solo i risultati della ricerca e non l'informazione, che resta presente sul sito sorgente, ma viene nascosta a seguito della deindicizzazione o cancellazione dei link. Come osservato da P. Sammarco, *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, in E. Tosi (a cura di), *Privacy digitale,* cit., 174, si tratta, dunque, di "un diritto affievolito rispetto all'oblio vero e proprio, perché si sostanzia nel diritto a non essere reperiti facilmente nel mondo della rete attraverso l'interrogazione dei motori di ricerca".

[44] In *Foro it.*, 2019, I, 227.

tra diritto all'oblio (posto a tutela della riservatezza della persona) e diritto di cronaca (posto al servizio dell'interesse pubblico all'informazione), ha rimesso alle Sezioni Unite la questione riguardante l'assetto dei rapporti tra gli stessi.

In particolare, nel provvedimento si legge che è necessario "a) individuare (univoci criteri di riferimento che consentano di conoscere) i presupposti in presenza dei quali un soggetto ha diritto a richiedere che una notizia che lo riguarda, legittimamente diffusa in passato, non resti esposta a tempo indeterminato alla possibilità di nuova divulgazione, e b) precisare in che termini l'interesse pubblico alla ripubblicazione di vicende personali faccia recedere il diritto all'oblio in favore del diritto di cronaca".

Le Sezioni Unite, con una pronuncia del 22 luglio 2019[45], mutando la prospettiva dell'analisi rispetto all'ordinanza di rimessione, si sono orientate nel senso della necessità di operare, nel caso in questione[46], un bilanciamento del diritto all'oblio non con il diritto di cronaca, bensì con il diritto alla "rievocazione storiografica" di eventi passati. La Corte ha, quindi, affermato che "in tema di rapporti tra diritto alla riservatezza (nella sua particolare connotazione del c.d. diritto all'oblio) e diritto alla rievocazione storica di fatti e vicende concernenti eventi del passato, il giudice di merito – ferma restando la libertà della scelta editoriale in ordine a tale rievocazione, che è espressione della libertà di stampa e di informazione protetta e garantita dall'art. 21 Cost. – ha il compito di valutare l'interesse pubblico, concreto ed attuale alla menzione degli elementi identificativi delle persone che di quei fatti e di quelle vicende furono protagonisti. Tale menzione deve ritenersi lecita solo nell'ipotesi in cui si riferisca a personaggi che destino nel momento presente l'interesse della collettività, sia per ragioni di notorietà che per il ruolo pubblico rivestito. In caso contrario, prevale il diritto degli interessati alla riservatezza rispetto ad avvenimenti del passato che li feriscano nella dignità e nell'onore e dei quali si sia ormai spenta la memoria collettiva".

---

[45] Cit. *supra*, nota 5.

[46] Si trattava della rievocazione, da parte di un quotidiano, di un omicidio avvenuto ventisette anni prima, il cui responsabile aveva scontato la relativa pena detentiva e si era reinserito positivamente nel contesto sociale. Per i primi commenti alla sentenza delle Sezioni Unite, v. G. Finocchiaro, *Le Sezioni Unite sul diritto all'oblio*, in *Giust. civ*., 29 luglio 2019, nonché V. Cuffaro, *Una decisione assennata sul diritto all'oblio*, in *Corr. giur*., 2019, 1189 ss., il quale mostra di apprezzare tale sentenza sia per la "qualità della soluzione adottata", sia per il "metodo". In senso critico nei confronti della stessa, v., invece, D. Muscillo, *Oblio e divieto di lettera scarlatta,* in *Danno e resp*., 2019, 611 ss. Manifestano perplessità sulla scelta operata dalle Sezioni Unite anche A. Bonetta, *Diritto al segreto del disonore. "Navigazione a vista" affidata ai giudici di merito*, *ivi*, 614 ss., e G. Calabrese, *Rievocazione storica e diritto all'oblio*, *ivi*, 620 ss., secondo il quale, in particolare, la Cassazione avrebbe perso l'occasione di fare chiarezza, "portando la questione su altri lidi (la rievocazione storica e la storiografia), che appaiono, in realtà, non del tutto pertinenti rispetto alla questione di fondo".

Tale decisione è stata attesa con ansia, soprattutto in considerazione del fatto che l'art. 17 del Regolamento 2016/679, pur avendo finalmente riconosciuto esplicitamente l'esistenza del "diritto all'oblio"[47], non solo lo ha fatto nella limitata prospettiva di un "diritto alla cancellazione" dei dati[48], ma non è arrivato neppure a tutelarlo quale diritto incomprimibile (risultando lo stesso suscettibile di subire rilevanti limitazioni legate alla libertà di espressione, al pubblico interesse, nonché agli interessi storici, statistici e di ricerca scientifica[49]), e, soprattutto, ha rinunciato a precisare i confini tra quel diritto, da un lato, e le libertà e gli interessi sopra indicati, dall'altro.

Non pare, però, che l'intervento delle Sezioni Unite sia da considerare senz'altro sufficiente a sopire i numerosi dubbi legati alla disciplina del diritto all'oblio, dei quali difficilmente ci si libererà in mancanza di un intervento chiarificatore del legislatore[50]. In effetti, di là del fatto che – come non si è mancato di osservare[51] – tale pronuncia finisce col lasciare sostanzialmente irrisolto il problema del confine tra diritto all'oblio e diritto di cronaca, dalla lettura del Regolamento Europeo emerge comunque un contrasto netto tra la previsione di cui all'art. 17, insomma priva di quel carattere innovativo che invece ci si aspet-

---

[47] Per R. Senigaglia, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale,* in *Nuove leggi civili commentate*, 2017, 1023 ss., il diritto all'oblio "è conformato come diritto soggettivo tipico dal reg. UE 2016/679". In senso critico nei confronti della scelta operata con tale Regolamento, v., peraltro, F. Di Ciommo, *Il diritto all'oblio,* cit*.,* 306 ss. In senso analogo, v. V. D'Antonio, *Oblio e cancellazione dei dati nel diritto europeo*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina, cit.,* 2016, *passim*, nonché D. Barbierato, *op. cit.,* 2100 ss.

[48] Quindi, tutto sommato, riduttivamente (così, F. Di Ciommo, *Oblio e cronaca: rimessa alle Sezioni Unite la definizione dei criteri di bilanciamento*, in *Corr. giur*., 2019, 5 ss., e D. Barbierato, *op. cit*., 2100 ss.). Parla di "forse indebita sovrapposizione dei termini oblio e cancellazione" A. Thiene, *op. cit.*, 426, la quale riconosce, peraltro, al Regolamento Ue il merito di aver previsto un ventaglio di ipotesi (v. paragrafo 1 dell'art. 17) "variegato ed esaustivo", dalle quali emergerebbe il "trionfo della c.d. autodeterminazione informativa".

[49] V., infatti, il paragrafo 3 dell'art. 17.

[50] Almeno ad una parte delle perplessità relative alla effettiva portata delle disposizioni in materia di diritto all'oblio, ha, comunque, tentato di fornire risposta, di recente, la Corte di Giustizia Ue (Corte Giustizia Ue, grande sezione, 24.9.2019, n. 136, in *Dir. & Giust.,* 2019, 25 settembre), la quale ha stabilito che il gestore di un motore di ricerca è tenuto ad effettuare la deindicizzazione non in tutte le versioni del suo motore di ricerca, quindi a livello mondiale, ma solo nelle versioni di tale motore corrispondenti a tutti gli Stati membri. Secondo V. Cuffaro, *op. cit*., 1197, la Corte ha in tal modo finito col ridurre l'enfasi assegnata al diritto all'oblio quale poteva trarsi dalla sentenza della Corte relativa al caso Google Spain.

[51] Secondo D. Muscillo, *op. cit*., 611 ss., "se lo scopo dichiarato dalla sentenza è quello di fornire all'interprete una chiara linea di confine tra il diritto di cronaca e il diritto all'oblio, c'è da credere che l'obiettivo si stato mancato, perché la lettura della stessa ingenera più perplessità di quante contribuisca a risolverne".

tava arrivasse a connotare tale disposizione, e quanto stabilito nei Considerando 65 e 66 [52]. Il primo dei due Considerando riporta, infatti, una chiara distinzione tra "diritto di ottenere la rettifica dei dati personali e il diritto all'oblio", mentre il Considerando 66 fissa i principi "per rafforzare il diritto all'oblio", mediante l'estensione del diritto di cancellazione. Ma, a ben vedere, è proprio tale ultima disposizione a far emergere i limiti della scelta operata in materia in sede normativa, risultando il "diritto all'oblio" (forse non a caso relegato in parentesi nella rubrica dell'art. 17) inteso solo quale (ipotizzato) effetto dell'esercizio del "diritto alla cancellazione" (cui è invece immediatamente dedicata la rubrica della medesima norma): la realizzazione di quest'ultimo, però, non sempre comporta, in effetti, il pieno soddisfacimento anche del primo.

Appare evidente, allora, come il legislatore abbia perso l'occasione propizia per introdurre una disciplina equilibrata, coerente e soprattutto concretamente in grado di garantire – conformemente alle aspettative maturate nel corso degli ultimi anni e in più occasioni rivelatesi degne di attenzione e di necessaria tutela – la protezione dei soggetti titolari dei dati, soprattutto ove il relativo trattamento avvenga mediante la rete Internet e, in particolar modo, ove lo stesso riguardi informazioni relative ai minori.

Non è chiaro, d'altro canto, se l'art. 17 possa consentire, almeno nel caso di trattamento illecito, oltreché di adottare i provvedimenti urgenti e cautelari, anche di infliggere le sanzioni amministrative e pecuniarie previste dall'art. 83, paragrafo 5, lett. b, nonché di applicare le misure coercitive indirette di adempimento di cui all'art. 614 *bis* c.p.c. [53]. Inoltre, come non si è mancato di osservare [54], resterebbe da chiarire se, in caso di pregiudizi morali, al risarcimento del danno possa essere attribuita una funzione diversa da quella compensativa. Soprattutto ove si tratti di lesioni riguardanti i diritti fondamentali dei minori, sembra, in effetti, che la eventuale funzione sanzionatoria del risarcimento sia destinata a rivelarsi maggiormente idonea a contribuire a garantire effettività alle regole previste dal Regolamento [55].

---

[52] In proposito, v. D. Barbierato, *op. cit*., 2100 ss.

[53] In senso favorevole alla relativa utilizzazione, v. Trib. Rieti, cit. *supra*, nota 23.

[54] A. Thiene*, op. cit*., 444.

[55] Sul punto, v. E. Andreola, *Minori*, cit., 14 ss., secondo la quale, "nel caso dell'illecito digitale potrebbe essere maggiormente garantista un approccio semplificato, rinvenendo in tale illecito la figura discussa di danno non patrimoniale *in re ipsa* in cui il danneggiato è onerato (soltanto) della prova del *quantum*".

5. Il consenso del minore nel d.lgs. n. 101 del 10-08-2018 e la generale tendenza alla valorizzazione della sua volontà

Il d.lgs. n. 101/2018 – al di là della relativa significativa portata in ordine alla disciplina del trattamento dei dati personali – offre senz'altro uno stimolante spunto di riflessione pure riguardo alla più ampia questione concernente la rilevanza da attribuire, in generale, alla volontà del minore.

Per quanto concerne la disciplina dettata in materia dal nostro legislatore, occorre, innanzitutto, fare riferimento alla legge 4 maggio 1983, n. 184, modificata dalla legge 28 marzo 2001, n. 149. Ai sensi di tale normativa, nel corso del procedimento per la dichiarazione di adottabilità, in caso di affidamento preadottivo e al momento della dichiarazione di adozione, deve sempre essere sentito sia il minore che abbia compiuto i dodici anni, sia il minore di età inferiore in considerazione della sua capacità di discernimento (v. artt. 10, ult. co., 15, co. 2, 22, co. 6, 23, co. 1, 25, co. 1).

L'obbligatorietà dell'ascolto del minore ultra-dodicenne o anche di età inferiore purché dotato di sufficiente capacità di discernimento è stata pure sancita con riferimento alle procedure contenziose di separazione e divorzio e a quelle relative all'affidamento di figli nati fuori del matrimonio (337-*octies* c.c., introdotto dal d.lgs. 28 dicembre 2013, n. 154) [56].

La riforma del 2012 in materia di filiazione ha, del resto, esteso a tutte le procedure giudiziarie il diritto del minore ad essere ascoltato, come si evince dalla disposizione generale di cui all'art. 315 *bis* c.c., relativo ai "Diritti e doveri del figlio" [57].

Coerentemente, oggi, l'"ascolto" dei minori, già previsto nell'art. 12 della Convenzione di New York sui diritti del fanciullo, si reputa rappresentare un adempimento assolutamente necessario nelle procedure giudiziarie che li riguardino e, in particolare, in quelle relative al loro affidamento ai genitori, ai sensi dell'art. 6 della Convenzione di Strasburgo, nonché, appunto, dell'art. 315

[56] Per un'analitica rassegna della disciplina dell'"ascolto" del minore nell'ordinamento giuridico nazionale e sovranazionale, v. M. Piccinni*, op. cit.,* 410 ss., nonché, più di recente, G. Dosi, *Ascolto del minore,* in *Lessico di Diritto di famiglia*, 2017, 89 ss.

[57] G. Recinto e F. Dell'Aversana, *op. cit*., 38 ss., osservano come la previsione di cui all'art. 315 *bis* c.c., sebbene "molto apprezzabile", "almeno nelle intenzioni", "per come modellata e concepita" non risulti, però, "funzionale a far emergere le concrete attitudini ed esigenze del minore stesso. Ed, invero, nell'art. 315 *bis* c.c. il diritto all'ascolto è ancorato alle «questioni e le procedure» che riguardano il minore di età". "Tuttavia" – precisano gli aa. – "forse preliminarmente sarebbe stato opportuno fissare – senza limiti di età ovviamente in quanto il linguaggio può essere anche non verbale – il diritto del minore ad essere ascoltato in famiglia e in ogni altra formazione sociale ove svolge la sua personalità, quali luoghi fisiologici e naturali di manifestazione dei suoi bisogni, delle sue capacità, delle sue istanze".

bis c.c. (introdotto dalla legge n. 219 del 2012) e degli artt. 336 *bis* e 337 *octies* c.c. (inseriti dal d.lgs. n. 154 del 2013) [58].

Insomma, la linea di tendenza sembra univocamente nel senso della finalizzazione dell'ascolto del minore alla valorizzazione della sua personalità e della sua autonomia nelle scelte esistenziali [59].

Senz'altro peculiare, allora, si presenta la posizione di chi, pur essendo minorenne, abbia già compiuto i 16 anni e, in alcuni casi, anche solo i 14.

Significativa sembra, al riguardo, la recente decisione del Tribunale per i Minorenni di Caltanissetta [60], secondo il quale la valorizzazione della volontà del minore nubendo, alla luce della *ratio* della Convenzione europea sull'esercizio dei diritti dei minori, impone al giudice di interpretare restrittivamente la nozione di "gravi motivi" di cui all'art. 84 c.c., nel senso che l'autorizzazione a contrarre matrimonio anteriormente al conseguimento della maggiore età possa essere negata nei soli casi in cui si accerti in concreto che il minore abbia subito un significativo condizionamento della propria sfera intellettiva e/o volitiva, tale da far ritenere che la manifestazione di volontà per conseguire l'autorizzazione a contrarre matrimonio espressa dallo stesso minore sia stata viziata.

Del resto, anche il Tribunale di Roma, con il citato provvedimento del 23.12.2017 [61], si è pronunciato, in via di principio, in senso sostanzialmente analogo. Secondo i giudici, ai "c.d. grandi minori (quelli che abbiano raggiunto 16 anni, e in alcuni casi 14 anni di età) va attribuito ampio margine di autodeterminazione". Più specificamente, "i minori possono essere distinti" – nell'ottica dei giudici di Roma, che richiama espressamente una terminologia adottata nel diritto francese (ma non ignota anche nella nostra esperienza) – in "cd. *petits enfants* e *cd. grands enfants*", laddove "per i primi, prevale l'esigenza di protezione; per i secondi, l'esigenza di esercitare i diritti di libertà". "Nella seconda categoria", conclude il Tribunale, "certamente si annovera il sedicenne il quale,

---

[58] Così: Cass. 31.3.2014, n. 7478, in *Foro it.* 2014, I, 1471; Cass. 10.9.2014, n. 19007, in *Foro it.* 2014, I, 3077; Cass. 26.3.2015, n. 6129, in *Foro it.* 2015, I, 1543; Cass. 21.4.2015, n. 8100, in *Diritto & Giustizia,* 2015, 22 aprile; Cass. 9.6.2015, n. 11890, in *www.giustiziacivile.com,* 2016, 11 gennaio; Cass. 12.5.2016, n. 9780, in *Diritto & Giustizia,* 2016, 13 maggio; Cass. 7.3.2017, n. 5676, in *Foro it.,* 2017, I, 1211; Cass. 27.3.2017, n. 7762, in *www.Ilfamiliarista.it,* 15 giugno 2017.

[59] Si ricordino, in particolare, Cass. 26.3.2010, n. 7282, in *Giust. civ. mass.,* 2010, 438, e Cass. 5.3.2014, n. 5097, in *Foro it.* 2014, I, 1067. Sul punto, v. le considerazioni svolte in E. Quadri, *op. cit*., 281 e *passim* (e *I figli nel conflitto familiare,* in *Genitori e figli: quali riforme per le nuove famiglie*, Ipsoa, 2013, 211 ss.), nonché, in particolare, le osservazioni di E. La Rosa, *op. cit*., 206.

[60] Trib. Min. Caltanissetta, 26.10.2017, in *Nuova giur. civ. comm*., 7-8/2018, con nota di F. Scia, *La volontà del minore ed i "gravi motivi" di cui all'art. 84 cod. civ,* cui si rinvia per un approfondimento della questione concernente, in generale, la rilevanza della volontà del minore.

[61] V. *supra*, nota 23.

infatti, riceve già dalle norme vigenti un trattamento differenziato" [62].

Sintomatico, con riferimento ai tempi di frequentazione dei genitori da parte del figlio che abbia compiuto 15 anni, risulta come il Tribunale di Torino [63] si sia pronunciato per l'assorbente rilevanza della volontà espressa dal medesimo in sede di ascolto.

La soluzione adottata dal legislatore con il d.lgs. n. 101/2018 sembra, allora, sostanzialmente allineata alla progressiva e trionfante tendenza, che emerge sia a livello legislativo, sia a livello giurisprudenziale, nel senso di valorizzare la volontà dei minori, soprattutto una volta compiuto il quattordicesimo anno di età. Del resto, a quattordici anni il minore è chiamato a rispondere personalmente anche in sede penale delle proprie azioni.

Inoltre, l'abilità con la quale i minori (perfino i bambini!) sono in grado di navigare in Internet e comunicare online, nel denotare una decisa, per così dire, "maturità digitale" – essendo gli stessi in grado di barcamenarsi tra siti e applicazioni varie con una dimestichezza che spesso nemmeno gli adulti dimostrano di possedere – avrebbe reso, tutto sommato, poco coerente e, soprattutto, non aderente alla realtà l'eventuale scelta del legislatore di confermare il limite anagrafico dei sedici anni prescritto dal GDPR.

Non tutti, peraltro, concordano circa la opportunità di abbassare il limite di età: i minori infra-sedicenni non avrebbero, infatti, secondo alcuni [64], la maturità sufficiente per comprendere fino in fondo il significato di certe offerte commerciali e, più in generale, per cogliere i rischi connessi all'uso della rete Internet.

Ferma restando la piena condivisibiltà delle preoccupazioni legate ad un uso indiscriminato della rete da parte dei minori, il più alto limite dei 16 anni, oltreché, nella prospettiva accennata dianzi, esorbitante in un contesto sociale caratterizzato dalla tendenza irrefrenabile all'uso di Internet da parte perfino dei preadolescenti, sembra presentarsi, d'altro canto, almeno di per sé, comunque tutt'altro che sufficientemente idoneo a garantire l'acquisizione di un consenso se-

---

[62] Del resto, questo è l'orientamento che emerge da numerose sentenze di merito (e v., ad esempio, Trib. Milano, 14.4.2014, citato da E. Andreola, *La tutela del figlio sedicenne nei social network usati dai genitori,* in *www.rivistafamilia.it*, *2018*). Anche il recentissimo provvedimento del Tribunale di Rieti, cit. *supra*, nota 23, richiama la differenza tra le due diverse categorie di minori.

[63] Trib. Torino, decr. 4.4.2016, in *Ilfamiliarista.it,* 3 gennaio 2017.

[64] In proposito, v. A. Thiene, *op. cit.*, 422, la quale condivide la scelta operata dal Regolamento europeo di fissare a 16 anni il limite di età, considerata "la coincidenza della previsione europea con la regola contenuta all'art. 108 l. 22 aprile 1941, n. 633, a protezione del diritto d'autore". "Nel mondo virtuale" – precisa, infatti, l'a. – "l'utente costruisce il proprio profilo combinando insieme non solo informazioni di vario genere…ma anche fotografie e video, al punto che questo vero e proprio sistema di possibilità creative potrebbe rendere non troppo audace la similitudine tra la personalizzazione di una pagina web e l'opera dell'ingegno".

riamente informato e consapevole da parte del minore e, quindi, ad offrire allo stesso una concreta tutela dei relativi interessi.

Non si può, allora, fare a meno di ritenere che la soluzione per una effettiva protezione di tutti i minori che navigano in Internet non risieda tanto e solo nella scelta, da considerarsi peraltro imprescindibile, di fissare un ragionevole limite di età per l'accesso ai servizi della società dell'informazione, bensì nell'impiego da parte dei fornitori di servizi e delle piattaforme social di meccanismi tecnologici destinati a precludere ai minori stessi la possibilità di attivare operazioni potenzialmente dannose.

Sarebbe, allora, forse il caso – anche alla luce dei diversi interventi della Commissione europea e del Parlamento [65], finalizzati a sensibilizzare gli stati membri e a spingerli ad adottare misure idonee a far fronte ai rischi legati all'uso spesso indiscriminato della rete da parte dei minori – di insistere sulla necessità della formazione dei minori stessi in ordine alle competenze relative ai mezzi di informazione, della educazione ai media, con inserimento di tale materia nei programmi scolastici, della alfabetizzazione digitale e mediatica dei minori e dei loro genitori, della formazione digitale continua per gli educatori che lavorano su base permanente con gli alunni nelle scuole, nonché, come pure espressamente previsto dal Parlamento europeo [66], di una "alleanza nel settore dell'istruzione fra famiglie, scuola, società civile e parti interessate, compresi i soggetti operanti nei media e nei servizi audiovisivi, per garantire una dinamica equilibrata e proattiva tra mondo digitale e minori" [67].

Quanto, poi, agli strumenti per consentire una corretta ed inequivocabile identificazione dei genitori tenuti a prestare il loro necessario consenso in luogo del minore, come si è già avuto modo di osservare, sarebbe senz'altro auspicabi-

---

[65] V., infatti, la Proposta di risoluzione del Parlamento europeo sulla tutela dei minori nel mondo digitale del 24 ottobre 2012, in *http://www.europarl.europa.eu.*

[66] V. *supra*, nota 65.

[67] In tale ordine di idee si muove C. Perlingieri, *Gli accordi,* cit., 119, la quale osserva come la soluzione vada ricercata in una "strategia pluridimensionale", basata "su strategie di sensibilizzazione fondamentali per assicurare la partecipazione attiva dei minori" (ad es., mediante "l'introduzione di nozioni di base sulla protezione dei dati nei programmi scolastici"), nonché "su un trattamento equo e lecito dei dati personali" degli stessi (ad es., "mediante la rinuncia a chiedere i dati sensibili nel modulo di iscrizione"), "sull'attuazione di tecnologie a difesa della *privacy* dei minori" (per es., mediante "software per la verifica dell'età") e "sull'autoregolamentazione dei fornitori di *social networks*" (ad es., mediante la previsione di sanzioni disciplinari per incentivare il rispetto delle buone pratiche). Sotto quest'ultimo profilo, la stessa a., in *La tutela dei minori,* cit.*,*1327 ss., passa analiticamente in rassegna gli strumenti di autoregolamentazione adottati dal 1998, anno al quale risale il Codice di autoregolamentazione per i servizi in Internet, al 2016, quando, su sollecitazione dell'UE, è stato adottato un Codice di condotta sottoscritto da aziende informatiche come Facebook, Microsoft, Twitter e YouTube (Google), le quali si sono proposte l'obiettivo di osteggiare la diffusione dell'illecito incitamento all'odio on line in Europa.

le la predisposizione, sulla falsariga di quanto stabilito negli Stati Uniti [68], di un sistema di controllo mirato, basato, ad esempio, sulla richiesta del pagamento di una somma simbolica (0,01 cent.) al titolare del trattamento tramite transazione bancaria, con l'onere di precisare, nell'indicazione della causale, che il titolare del conto è anche il titolare della responsabilità genitoriale. Diversamente, si potrebbe optare per la connessione tramite video conferenza del genitore col personale addetto alla piattaforma, o, infine, per la più semplice via dell'identificazione del genitore stesso per mezzo di un documento di identità [69].

In ogni caso, non pare sia possibile prescindere, ove si intenda tutelate adeguatamente gli interessi dei minori che si muovono nella rete, dalla attivazione di percorsi educativi e formativi destinati ad aumentare il livello di consapevolezza dei giovani internauti.

[68] V. *supra*, nota 13.

[69] Sul punto, v. I.A. Caggiano, *Privacy e minori*, cit., *passim*, la quale osserva come "il legislatore abbia perso l'occasione di indicare i criteri cui ispirarsi nei diversi canali di comunicazione in base al rischio per il minore": ad esempio, "possibili tipologie di controllo differenziato nell'acquisto di beni o servizi distinti per tipologia". "In quest'ottica", aggiunge l'a., "potrebbe oggi pensarsi, sempre con riguardo alle ipotesi che espongano a maggiori rischi per il minore, anche all'utilizzo di sistemi biometrici di identificazione del genitore (tramite impronte digitali, firma, riconoscimento facciale o iride)".

A GARDEN OF FORKING PATHS: THE SEVERAL AND MULTIFACETED PERSPECTIVES IN THE RELATIONSHIP BETWEEN PRIVACY AND TECHNICAL ENABLERS

Roberto Montanari e Sara Saleri

Abstract:

As in the short story written by Jorge Louis Borges "The Garden of Forking Paths", the multifaceted combinations between privacy and technological evolution display in front of us a multifaceted landscape, and uncountable set of links among data, technologies and privacy are echoing continuously several alternatives. Moving from this emblematic metaphor of current scenario, this paper intends to overview the strongest implications in terms of privacy induced by raising of big data related technologies, internet of things and blockchain.

Introduction

In the wide debate on privacy, even wider after the recent introduction of GDPR, the role of the technological enablers is among the "hottest" points. It is of course largely acknowledged how technologies are growing fast since the beginning of the digital age. What is actually and recently impressive is how the technological roadmaps, as well as the improvement in their functional capabilities, are stimulated and fed by the raising of the big data. [1] In brief, the amount of data availability, every given year after 2014, seems to be larger than the amount of data managed by the entire world from the previous year till the be-

[1] See V Mayer-Schönberger and K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).

ginning of the human history. And this is only one, and may be not the most relevant, of the data revolutionary related aspects.

Therefore, data and technologies are deeply entitled, and it goes without saying how this chain would influences and modify privacy, and of course its regulatory framework. Same happen for other relevant technological players which are changing the game field in privacy. For instance, Internet of Things, i.e. the possibility to address a telematic identity to all things around us, is multiplying possibilities to control everything from everything, to assess what happen in every remote filed of our life, even in space. Blockchain, a revolutionary new way to handle payments and many other financial behaviours, is another big step toward a deeper digitalisation in every part of humans' life.

The intent of this paper is trying to start in outlining and retracing the wide set of paths in which data, privacy, and technologies are entitled. As in the short story written by the Argentine writer Jorge Louis Borges and titled 'The Garden of Forking Paths' ('El jardín de senderos que se bifurcan'), the landscape in front of the multiple combinations among data, technologies and privacy are echoing continuously several alternatives, that are appearing in front of us as soon as we set out among one of the identified path.

The shape in which we have tried to propose such scenario is a literature review to which we have approached following three main criteria. First of all, we have tried to consider trending and emerging topics, with a special focus on new technologies (such as blockchain or user-tracking technologies) which are likely to continue to impact Data Protection in the future; secondly, given the nature of Data protection and the speed of change and evolution, we have given preference to recent research; thirdly, to maximize the possibility to deepen and disseminate knowledge on the mentioned topics, our research focused mainly on Open Access content. [2]

This paper was drafted within the framework of the EU-Funded project "Training Activities to Implement the Data Protection Reform" (TAtoDPR), [3] which was aimed at preparing and training professionals to effectively perform the duties of Data Protection Officers (DPO) as outlined in the General Data Protection Regulation (Regulation 2016/679, known as GDPR).

More specifically, this review is part of the work that RE:Lab has undertaken to structure the Technical, Organizational and Impact Assessment (TOIA)

[2] The authors would like to sincere thank Andrea Castellano, Francesco Giacomello and Francesco Maria Riccio for their competent contribution to the paper's contents, and Doina Tiganu for her support in the editing.

[3] More precisely the TAtoDPR project has been co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020) under Grant Agreement n. 769191. For more information on the TAtoDPR project see: https://www.tatodpr.eu.

Module of the training courses, which was focused on the technical aspects of data creation, management and storing.

We have identified a series of topics that are central in the current literature and that could also be important for the DPO – the major protagonist of the project from which this paper take the move – and we have decided to focus our review on the three technological domains (briefly introduced above) which are predominant in our hyper-connected society and that have strong implications in terms of data protection, namely Big Data, Internet of Things and Blockchain.

1. Big Data: huge volume in data spread

If it is broadly recognized that Volume, Variety and Velocity (the so-called *Three Vs*) are the three main dimensions characterizing Big Data, [4] they also represent a challenge in terms of data protection. In a technical perspective, large data sets are particularly problematic in terms of data capturing, storage, analysis, [5] transfer, visualization, and of course privacy.

The challenges – together with the opportunities – implied by Big Data are approached by many authors from the company's perspective: Raguseo [6] investigates the adoption levels of big data technologies in companies, and the big data sources they use; Chluski & Ziora [7] and Sivarajah et al. [8] focus on application of big data solutions in the process of organizations' management; Elgendy & Elragal [9] and Kościelniak & Puto [10] have a more focused perspective on the

[4] See D Laney, *3-D data management: Controlling data volume, velocity and variety. Application Delivery Strategies by META Group Inc.* Retrieved from https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (2001, February 6). This definition has also been formalized in different kind of glossaries or official documents, such as the Tech America Foundation's Federal Big Data Commission, which states: 'Big data is a term that describes large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information'.

[5] A Gandomi, M Haier, 'Beyond the hype: Big data concepts, methods, and analytics' (2015) Vol. 35, Issue 2, International Journal of Information Management.

[6] E Raguseo, 'Big data technologies: An empirical investigation on their adoption, benefits and risks for companies' (2018) Vol. 38 Issue 1, International Journal of Information Management.

[7] A Chluski, L Ziora L, 'The role of big data solutions in the Management of organizations. Review of selected practical examples' (2015) Vol. 65, Procedia Computer Science.

[8] U Sivarajah et al., 'Critical analysis of Big Data challenges and analytical methods' (2017), Volume 70, Journal of Business Research 263-286.

[9] N Elgendy, A Elragal, 'Big Data Analytics in Support of the Decision Making Process' (2016), Volume 100, Procedia Computer Science 1071-1084

role of Big Data in decision-making processes.

Starting from the company's perspective doesn't mean that the individual's side is neglected: the sheer number and dimension of data available also exposes individuals to unprecedented privacy vulnerability, where organizations managing them are unprepared to do so correctly and effectively. [11] In particular, the issue of *profiling* activities is crucial: Big Data also means that companies have the chance to use automated data analysis and filter the amount of gathered data to understand customers and users, research and record their preferences, and gain a vantage point in addressing them commercially. Such practices require special attention, as they might threat privacy when incorrectly performed.

Some studies focus on concrete case studies in contexts where the impact of Big Data on privacy issues cannot be underestimated. Logica and Magdalena for example, point their attention on the academic realm, in particular on the application of Big Data to e-Learning. [12] The medical, biomedical and healthcare fields, instead, are the main focus of the study by Abouelmehdi et al.: [13] as they point out, while Big Data is being hailed as the key to improving health outcomes, gain valuable insights and lowering costs, the security and privacy issues are so overwhelming that healthcare industry is unable to take full advantage of it with its current resources.

More analytically, a number of investigations focus on how to reduce the risk of breaching the privacy of individuals. Katal et al. examine the circumstances under which the individuals' privacy might be breached, [14] while Matturdi et al. introduce the concept of privacy protection in big data. [15]

To better understand the implications of big data in terms of privacy, it can be useful to focus on the different stages of a big data life cycle, as suggested by Mehmood et al.: data generation, data storage, and data processing. [16]

---

[10] H Kościelniak, A Puto, 'BIG DATA in Decision Making Processes of Enterprises'. (2015) 65. Procedia Computer Science' 1052-1058.

[11] See S Yu, 'Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data' (2016) Vol. 4, IEEE Access.

[12] B Logica, R Magdalena, 'Using Big Data in the Academic Environment' (2015), Vol. 33, Procedia Economics and Finance.

[13] K Abouelmehdi et al., *Big data security and privacy in healthcare: A Review* (EUSPN 2017).

[14] M Katal, M Wazid, and RH Goudar, 'Big data: Issues, challenges, tools and good practices' (2013) Proc. IEEE Int. Conf. Contemp. Comput 404-409.

[15] B Matturdi et al, 'Big data security and privacy: A review' (2014) Vol. 11, n. 14, China Commun 135-145.

[16] A Mehmood et al., 'Protection of Big Data Privacy '(2016), Vol. 4, Special Section: Theoretical Foundations for Big Data Applications: Challenges and Opportunities, IEEE Access.

During the first stage – *data generation* –, as underlined also by Xu et al., [17] the risk of privacy violation can by minimized either restricting access or by falsifying data, for example through tools such as *Socketpuppet*, which conceals individual's activities online by creating a false identity, or *MaskMe*, which alows users to create aliases of their personal information, such as email address or credit card number.

As it concerns the *data storage phase*, the main approaches to preserve the user's privacy in this phase are: Attribute based encryption; [18] Identity based encryption; [19] Homomorphic encryption; [20] Storage path encryption; [21] usage of hybrid clouds. [22]

The last phase of big data cycle, *privacy protection in data processing*, according to Mehmood et al., should be analytically divided into two sub-phases.

In the first one, the goal is to safeguard information from unsolicited disclosure because the collected data may contain sensitive information about the data owner. In this case, the main strategy consists in anonymization techniques: generalization, suppression, anotomization, permutation, perturbation. [23] However, due to the availability of huge volumes of data and powerful data analytic tools, the existing anonymization techniques are becoming increasingly ineffective. Some researches for example indicate that simply anonymized data sets can be easily attacked in terms of privacy. De Montjoye et al. [24] collected a 15-months mobility dataset of 1.5 million people. After a simple anonymization operation (removing the obvious identifiers, such as name, home address, phone number, and staff ID), they obtained a data set where the location of an individ-

---

[17] C Xu et al., 'Information security in bigdata: Privacy and data mining' (2014) Vol. 2, IEEE Access 1149-1176.

[18] See: V Goyal et al., '*Attribute-based encryption for fine-grained access control of encrypted data' (2006)* Proc. ACM Conf. Comput. Commun. Secur 89–98; J Bethencourt, A Sahai, and B Waters, '*Ciphertext-policy attribute- based encryption'* (2007) Proc. IEEE Int. Conf. Secur. Privacy 321–33.

[19] X Boyenand, B Waters, 'Anonymous hierarchical identity-based encryption -without random oracles' (2006) vol. 4117, Proc. Adv. Cryptol. (ASIACRYPT) 290–307.

[20] C Gentry, *A fully homomorphic encryption scheme* (Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009)

[21] C Hongbing et al., 'Secure big data storage and sharing scheme for cloud tenants' (2015) Vol. 12, n. 6, China Commun. 106-115.

[22] X Huang and X Du, 'Achieving big data privacy via hybrid cloud' (2014) Proc. Int. Conf. INFOCOM512–517.

[23] See BCM Fung et al., 'Privacy-preserving data publishing: A survey of recent developments' (2010) Vol. 42, n. 4, ACM Comput. Surv, Art. no. 14.

[24] A de Montjoye et al., 'Unique in the crowd: The privacy bounds of human mobility' (2013), Vol. 3, Sci. Rep., Art. n. 1376.

ual was specified hourly with a spatial resolution equal to that given by the carrier's antennas. From the processed data set, they were able to identify a person with 95% accuracy by only four spatial-temporal points. The weakness of simple anonymization was later further confirmed by a similar test. [25]

Even if the level of anonymization is higher (for example combining different techniques, as suggested by Mehta & Rao [26]), another criticism arises in the second moment of data processing, which goal is to extract *meaningful information* from the data without violating the privacy. First of all, how can we extract useful information in the overwhelming abundance of data characterizing our era? How can we obtain valuable inputs from anonymized data, without losing information? In order to distinguish relevant data from irrelevant data, analytics comes into play to help organizations select the amount and type of information they require. There are several techniques proposed to analyze large-scale and complex data, which can be broadly grouped into: clustering, [27] classification [28] and association rule-based techniques. [29]

But selecting the right information does not, on its own, suffice to truly unleash the potential benefits it might produce: visualization is sometimes just as important for the exploitation of data as the analysis behind it.

Information visualization, the art of representing data in a way that is easy to understand and to manipulate, can help us make sense of information and thus make it useful. From business decision-making to simple route navigation, there's a huge (and growing) need for data to be presented so that it delivers value. [30] Information visualization plays an important role in making data digestible and turning raw information into actionable insights. It draws from the fields of human-computer interaction, visual design, computer science, and cognitive science, among others. Examples include world map-style representa-

---

[25] A. de Montjoye et al., 'Unique in the shopping mall: On the reidentiability of credit card metadata' (2015), Vol. 347, n. 6221, Science 536-539.

[26] BB Mehta, UP Rao, 'Privacy Preserving Unstructured Big Data Analytics: Issues and Challenges' (2016) Vol. 78, Procedia Computer Science.

[27] See: D. Feldman, M. Schmidt, and C. Sohler, 'Turning big data into tiny data: Constant-size core sets for k-means, PCA and projective clustering' (2013) Proc. ACM-SIAM Symp. Discrete Algorithms 1434–145; AS Shirkhorshidi et al., 'Big data clustering: A review' (2014), Proc. Int. Conf. Comput. Sci. Appl. 707-720.

[28] See: S. Agrawal, J.R. Haritsa, 'A framework for high-accuracy privacy-preserving mining' (2005) Proc. 21st Int. Conf. Data Eng. 193–204; G. Weiping, W. Wei, and Z. Haofeng, 'Privacy preserving classification mining' (2006) Vol. 43, n. 1, J. Comput. Res. Develop 39-45.

[29] CKS Leung, R.K. MacKinnon, and F Jiang, 'Reducing the search space for big data mining for interesting patterns from uncertain data' (2014) Proc. Int. Conf. Big Data 315-322.

[30] M. Kahn, 'Data and Information Visualization Methods, and Interactive Mechanisms: A Survey' (2011) International Journal of Computer Applications.

tions, line graphs, and 3-D virtual building or town plan designs.

Visualization methods are considered to be very important for the users' because they provide mental models of the information. [31] Visualization techniques make huge and complex information intelligible and serve as a visual user interface to provides insight of information to the user. [32] According to Ware, [33] the basic purpose of visualization is to create interactive visual representations of the information that exploit human's perceptual and cognitive capabilities of problem solving. In order to meet the requirement of maintaining a low workload for the user and increase the information effectiveness, generic guidelines [34] on info-view suggest to: work on Hierarchical representation of information; minimize the use of 3-dimensional representations; coordinate multiple views; allow an interactive navigation of the data; use them to support the user task.

Visualization techniques, thus, can enhance informed decision-making and data-driven strategies within public and private organizations. In this perspective, Data is not only seen as an individual's resource in need of protection, but also as a collective good, whose conscious exploitation can lead to better decision and policy-making, thus reverberating positive effects on end-users as well.

2. Internet of Things: every little thing they do is magic

One of the greatest present and future challenges to Data Protection is posed by the so-called Internet of Things (IoT). Expanding digitalization of objects and places, accompanied by the transfer of an enormous volume of data, put into question the effectiveness of existing measures for the protection of personal data, while demanding organizations involved to pay greater attention to Data Protection than ever before.

According to the review undertaken by Perera et al., [35] this challenge is clearly perceived by the users, who are becoming increasingly aware and concerned of possible threats to privacy implied by the pervasive IoT. A research from

[31] See C. North, *Information Visualization* (Center for Human-Computer Interaction, Department of Computer Science Virginia Polytechnic Institute and State University Blacksburg, VA 24061 USA, 2017).

[32] See R. Spence, *Information Visualization* (Addison-Wesley 2001).

[33] C. Ware, *Information Visualization: Perception for Design* (Morgan Kaufmann C 2004)

[34] For example DA Carr, *Guidelines for Designing Information Visualization Applications*, 1999.

[35] C. Perera et al., 'Privacy of Big Data in the Internet of Things Era' (2015) Vol. 17, Issue 3, IT Professional.

2015 [36] even highlighted the fact that privacy concerns could be a significant barrier to the growth of IoT. According the survey conducted, about 60% of internet users have basic privacy awareness of IoT and they know that smart devices, such as smart TVs, fitness devices, and in-car navigation systems could collect personal activities data. The survey also revealed that 87% of internet users were concerned about the type of personal information collected.

Thus, in this scenario, the satisfaction of security and privacy requirements plays a fundamental role. According to Sicari et al., [37] such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore, a flexible infrastructure is needed able to deal with security threats in such a dynamic environment.

To tackle this issue, researchers have been focusing on various approaches enforcing security and privacy. Sahmim and Gharsellaouib, [38] in their review, present several techniques, such as encryption, obfuscation, anonymization, the so-called "Sticky policy" (which allows to attach privacy policies to data owners and drive access control decisions and policy enforcement), data segmentation.

Malina et al. [39] go more in depth, presenting a detailed assessment of the performance of the most used cryptographic algorithms on constrained devices that often appear in IoT networks. In particular, they evaluate the performance of symmetric primitives, such as block ciphers, hash functions, random number generators, asymmetric primitives, such as digital signature schemes, and privacy-enhancing schemes on various microcontrollers, smart-cards and mobile devices. Furthermore, they provide the analysis of the usability of upcoming schemes, such as the homomorphic encryption schemes, group signatures and attribute-based schemes.

---

[36] TRUSTe, *Internet of Things Industry Brings Data Explosion, but Growth Could be Impacted by Consumer Privacy Concerns* (TRUSTe Research, 29 05 2014. [Online]). Available: http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns/

[37] S. Sicari et al., 'Security, privacy and trust in Internet of Things: The road ahead' (2015) Vol. 76, Computer Networks.

[38] S. Sahmim, H. Gharsellaouib, 'Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review' (2017), Proceedings of the International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, 6-8 September 2017.

[39] L. Malina et al., 'On perspective of security and privacy-preserving solutions in the internet of things' (2016) Vol. 102 Computer Networks.

On the other hand, other researchers, such as Thierer,[40] advocate for a regulation that do not jeopardize the innovation potential of this technology, while Weinberg et al.[41] explore one of the central tensions of the IoT, i.e. convenience vs. privacy and secrecy.

The IoT environment is likely to exponentially grow in the future, thus widening the scope of Data Protection concerns related to it. In particular, clearer measures for user's consent to data treatment and data management policies must adapt to such an evolving context. Furthermore, cybersecurity issues connected with IoT in sensitive domains, such as smart grids, healthcare, transportation or domotics pose urgent challenges in terms of governance.

Also, EIoT (Enterprise Internet of Things) demands for increased awareness from managers as to the level of protection assigned to data. As highlighted by Dzung et al.,[42] in the past, systematic integration of countermeasures against cyberattacks often followed integration of IT components with some delay. As a result, current Industrial IoT systems are vulnerable to a variety of cyberattacks. To counter these security and privacy risks, as stated by Sadeghi Wachsmann, M. Waidner,[43] a holistic cybersecurity concept for Industrial IoT systems is required, that addresses the various security and privacy risks at all abstraction levels. This includes different aspects, such as platform security, secure engineering, security management, identity management, industrial rights management.

3. Blockchain: an in-course disruptive innovation since the Internet itself

Since its emergence in 2008, Blockchain technology has seen a sharp increase in popularity and use. Its innovative nature has led many observers to consider it as the most disruptive invention since the Internet itself. Its potential is undoubtedly enormous, whether already exploited or not, and likely to have

[40] A.D. Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation' (2013) Vol. 21, Issue 2 Richmond Journal of Law and Technology.

[41] B.D. Weinberg et al., '*Internet of Things: Convenience vs. privacy and secrecy' (2015)* Vol. 58, Issue 6 Business Horizons.

[42] D. Dzung et al., '*Security for industrial communication systems' (2005)* 93(6) Proceedings of the IEEE.

[43] A.R. Sadeghi, C. Wachsmann, M. Waidner, 'Security and Privacy Challenges in Industrial Internet of Things' (2005) DAC '15 Proceedings of the 52nd Annual Design Automation Conference, Article No. 54.

great implications for Data Management and Protection. Moreover, even though its most popular example, the Bitcoin currency, might be regarded as highly controversial, the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world, as pointed out by Crosby et al.[44] In practice, this technology consists in creating a continuously growing list of ordered records, which are called blocks, to form a digital ledger. Its peculiarity is the fact that this list is widely distributed within a peer-to-peer network, which automatically validates each new record.

Authors such as Huckle et al.[45] and Banerjee et al.[46] posit the potential for blockchain technology in facilitating secure sharing of IoT datasets (e.g. using blockchain to ensure the integrity of shared datasets) and securing either civilian or military IoT systems. Starting from similar considerations, Ouaddah et al.[47] propose FairAccess as a new decentralized pseudonymous and privacy preserving authorization management framework that leverages the consistency of blockchain technology to manage access control on behalf of constrained devices. Indeed, access control is currently facing big challenges in the IoT world, since it is quite hard to implement current access control standards on smart objects due to their constrained nature. Here the blockchain technology might come to rescue, allowing for a reliable third party access handling.

Similarly, Angraal et al.[48] describe the possible use of the blockchain in the health-care sector, precisely because, offering a secure, distributed database that can operate without a central authority or administrator, it can provide a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing.

It is very important to notice how in all of the previous examples a fundamental role is played by the decentralization of the processes. This is because entitling a single institution to control a data flow corresponds inevitably to a security issue. On the other hand, blockchain allows for an egalitarian network-

---

[44] M. Crosby et al., 'BlockChain Technology: Beyond Bitcoin' (2016) Issue 2 Applied Innovation Review.

[45] S. Huckle et al., **'**Internet of Things, Blockchain and Shared Economy Applications', (2016) (Proceedings of the International Workshop on Data Mining in IoT Systems (DAMIS).

[46] M. Banerjee et al., *A blockchain future to Internet of Things security: A position paper* (Digital Communications and Networks, 2017).

[47] A. Ouaddahet al., *Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT,* (Europe and MENA Cooperation Advances in Information and Communication Technologies, 2017).

[48] S. Angraal et al., *Blockchain Technology Applications in Health Care,* (Circulation: Cardiovascular Quality and Outcomes, 2017).

ing system which relies on the users' community itself, since it becomes harder and harder to violate its mechanism the more copies of blockchain are distributed. Hence one could say that the power of this technology actually comes from the fact that it evades any possibility of a centralized management.

On this matter, we are due to notice the perspective of Scott, [49] who rises potential points of concerns such as the tech-from-above "solutionism" and conservative libertarian political dynamics of some of the technology start-up community that surrounds Bitcoin. The author considers "blockchain 2.0" technologies with more overtly communitarian ideals and their potential for creating "cooperation at scale". Again, this might provide us some remarkable insights, since this principle of cooperation is not just about ideals but could be crucial in order to manage security hazards.

Moreover, authors such as S. Raval and O'Reilly [50] state that decentralized applications (dapps) will become even more widely used than today's most popular web apps. Dapps are just applications that are executed on a peer-to-peer network, and thus existed well before the blockchain. However, it is argued how, implementing them with a blockchain mechanism, they will provide a more flexible, better-incentivized structure than current software models. As an example of a dapp exosystem, the authors describe the OpenBazaar decentralized market, and examine two case studies of dapps currently in use. Indeed, Huckle et al. [51] discuss how the IoT and blockchain technology can benefit shared economy applications, overtaking current shared economy applications such as Airbnb and Uber by creating a myriad of sharing applications, e.g. peer-to-peer automatic payment mechanisms, foreign exchange platforms, digital rights management and cultural heritage.

In the future, Data Protection Officers will be called to assess their compliance with existing national and international regulations: in this sense, they will have to consider the rising of new technologies such as that of blockchain-based Smart Contracts, which allow to enforce contracts remotely in a more trustable way. In conclusion, it should be kept in mind that, as with any new technology, the blockchain has to be considered with a critical attitude, even though it should be by construction a mechanism which guarantees a high level of dependability.

---

[49] B. Scott, *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?,* (prepared for the UNRISD Workshop Social and Solidarity Finance: Tensions, Opportunities and Transformative Potential" in collaboration with the Friedrich-Ebert Stiftung and the International Labour Office, Feb 2016).

[50] S. Raval, P O'Reilly, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology,* (Media, 2016).

[51] *op. cit*.

Conclusions: challenging regulatory framework and role of DPO

In the end, it appears clear how the metaphor chosen in the beginning of this paper looks relevant in understanding the current landscape where big data, IoT and Blockchain are not only influencing each other, and together are depicting a new frame for privacy, but as in the garden of forking paths, they are shaping every alternative, every possibility, in a kind of uncountable alternative producing mechanism.

These continuous transformations put in front of the DPOs and the regulators new challenges. The first have to cope in their daily work with these transformations, especially in trying to quickly understand which is the expect impact in organizations, data management and foreseeable risk for privacy and rules. The latter have to quickly understand what is happening around, which technologies are emerging and what of these technologies is concretely impacting on people and originations life. Of course, these challenges are enormous and require a wide view and quick capabilities to understand. In this paper, we have briefly outlined some technological players which are mature and relevant, but many other urgently require attention. Just one among the others: the role of Artificial Intelligent (AI), which is becoming to appear as a quite mature enabler. AI is hugely relevant in our scenario, another path full of forking paths, and it goes without saying that it could affect all the above-mentioned enablers, introducing a deeper level of autonomy and behavioral independence. DPO and regulators – from their different perspective – have to be tuned, even changing their interpretation framework in understanding transformations which are not only influencing privacy and data management but even more transforming intimately the nature of privacy and data management.

DOES PRIVACY BY DEFAULT MEAN RESEARCHERS SHOULD RECONSIDER RESEARCH ETHICS PRACTICE IN RELATION TO RECORDING INFORMED CONSENT

Alex Nunn

Abstract

It is normal practice for researchers collecting data from 'human subjects' to record that their participants have provided 'informed consent'. This often means recording personal data such as a name, address and signature when the underpinning research question – or in legal terms 'the specific purpose for processing data' does not actually require this. The provisions of GDPR in relation to 'privacy by default' might provide a rationale to revisit normal practice and ethical guidelines to give greater emphasis to anonymisation or pseudonymisation at the point of data collection. It is recommended that research organisations and researchers revisit normal practices and guidelines to consider where anonymised data collection might be utilised more fully.

1. GDPR a Summary

From May 2018, Europe's new data protection regime was significantly tightened with the introduction of the General Data Protection Regulation (GDPR). The impact of this regulation cannot be overstated – it touches all areas of organisational functions and substantially strengthens the rights of data subjects in relation to data controllers and processors. Proponents of GDPR suggest that for those already practicing strong data protection, the changes introduced by the GDPR are incremental. But even where incremental, some important challenges are thrown up by the changes.

The 99 articles of GDPR establish 8 rights for individuals: (1) to be informed, (2) access to the data held about them, (3) to have errors corrected, (4) to have their data erased, (5) to restrict aspects of data processing, (6) to be able to

move their data to a different organisation, (7) to object to the use of their data and (8) in relation to automated data profiling. GDPR ensures that organisations must have an appropriate 'legal basis' for collecting, storing and processing individuals' personal data and establishes the different possible grounds on which this may be constructed. For most organisations, these include consent, the delivery of a contractual services or to uphold the law in other respects or to protect 'vital interests' such as life preservation. [1]

The issue of consent is very familiar to researchers involved in collecting data. As with most extant guides and good practice in research ethics, consent in relation to GDPR must satisfy the criteria that it is given freely, is informed, specific and explicit. It must also relate to the collection, storage and use of the data, including any transfer of data between organisations. There are also specific measures related to children, with 'children' defined as those under the age of 18.

2. Research Ethics – The Position before the GDPR

Many of the principles of the GDPR are not new to researchers. As discussed below, the principles of informed consent, offering opportunities for withdrawal and early anonymisation of data are all well entrenched in good practice guidelines. For researchers, data protection usually arises in the context of 'research ethics'.

It is normal research practice in research involving human participants for details of the research design to be put in front of an ethics committee and be approved by that committee prior to any data being collected. For example, the UK Research Integrity Office suggests that

> *Researchers should submit research projects involving human participants, human material or personal data for review by all relevant ethics committees and abide by the outcome of those reviews. They should also ensure that such research projects have been approved by all applicable bodies, ethical, regulatory or otherwise.* [Section 3.7.9.] [2]

[1] Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> accessed 23 October 2019.

[2] UK Research Integrity Office, 'Code of Practice for Research' (2019) <https://ukrio.org/publications/code-of-practice-for-research/3-0-standards-for-organisations-and-researchers/3-7-research involving-human-participants-human-material-or-personal-data/> accessed 23 October 2019.

It is also normal that such ethics committees will require a sense of what questions the research will address, who will be involved and in what circumstances the research will be conducted. In practice, this involves submitting a summary of the research for approval, draft interview schedules or questionnaires, a sampling strategy and a plan for the ways that data will be collected including locations and timeframes. Prior to the GDPR, this usually included an 'informed consent' sheet to be given to research participants making them aware of the use of their data and how to withdraw from the research. In research projects where participants are at risk of some immediate harm – such as in clinical trials, these standards are particularly tight, but they are also applied to research investigating social or political issues. For example, the Social Research Association's Ethical Guidelines, currently dating from 2003 but due for review in 2019, state that informed consent "should ideally be both ORALLY and in WRITING", [3] emphasis in the original]. While many guidelines stop short of determining how consent should be recorded – this too has tended to be in writing, though most ethics guides stop short of mandating this. For example, the Economic and Social Research Council online Research Ethics Framework includes a 'Frequently Asked Question': "Is written consent always necessary?" which includes the following answer:

> *It is sometimes argued that formal written consent is not necessary because by consenting to see the researcher, a participant is in fact giving consent. However, it is good practice where possible for all participants to be provided with information giving the name and status of the researcher carrying out the study, a brief rationale of the study (including its purpose and value), and an account of why the individual is being invited to take part.*
>
> *The person interviewed should be made aware what will happen to the data, whether and how it may be shared with others, and whether they will be identified – and asked their preference.* [4]

At the same time, these various guidelines also imply that the responsibility to be able to demonstrate that consent has been gained belongs to the researcher. As such, despite this ambiguity in sectoral guidelines, most University ethical guidelines tend toward the default position that written consent is the expected norm, and that this is particularly the case where research involves risk and po-

[3] Social Research Association, 'Ethical Guidelines 2003' (2003) <https://the-sra.org.uk/common/Uploaded%20files/ethical%20guidelines%202003.pdf> accessed 23 October 2019.

[4] Economic and Social Research Council, 'Is Written Consent Always Necessary? - Research Ethics Framework Website' (2019) <https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/frequently-raised-questions/is-written-consent-always-necessary/> accessed 23 October 2019.

tential for harm, for instance by focussing on 'vulnerable' groups, such as young people, disabled people, or those experiencing social exclusion. Since social research frequently does focus on these groups, this is a common experience.

The default expectation then when researchers seek ethical approval for their data collection is that they will provide research participants with written information about the reasons for collecting data, how it will be stored, what analysis will be applied to it, how it will be placed in the public domain (e.g. confidentiality, anonymisation and pseudonymisation) and details about how they can withdraw. The right to withdraw in particular is often stressed as a condition for making abstract commitments to ensuring that consent is not a one-off process but an ongoing one, that may be subject to renegotiation. The Social Policy Association's guidelines are typical:

> *Consent to participate in a research study should be regarded as an on-going process and it should be made clear to participants that they are free to withdraw from the study or withhold information at any point. Participants should be given the opportunity to ask for further information about the study at any time.* [5]

This default position is also that researchers will secure written consent from their research participants. Here the University of Manchester's online guidance to staff researchers is illustrative. It suggests that consent can be gained in written or oral form but if it is the latter

> *Provided by asking the participant a series of questions (through the use of a consent script) and recording their verbal agreement to each statement. The recording can by done either by audio recording or through the use of detailed fieldnotes. If fieldnotes are used, you must include the participant's name, the date in which consent is being taken and the specific statements they are agreeing to. Please also note that if using this method you must provide justification to the ethics committee why this is needed.* [6]

What stands out here is both that not requiring written consent is to be regarded as an exception from the norm to be specially justified and that even where this is the case written notes of a participant name is required.

---

[5] Social Policy Association, 'SPA Guidelines on Research Ethics' (2019) <http://www.socialpolicy.org.uk/downloads/SPA_code_ethics_jan09.pdf> accessed 23 October 2019.

[6] University of Manchester, 'Preparing an Ethics Application' (2019) <https://www.staffnet.manchester.ac.uk/rbe/ethics-integrity/ethics/app-prep/#> accessed 23 October 2019.

3. Impact of Data Protection on Research Ethics Procedures

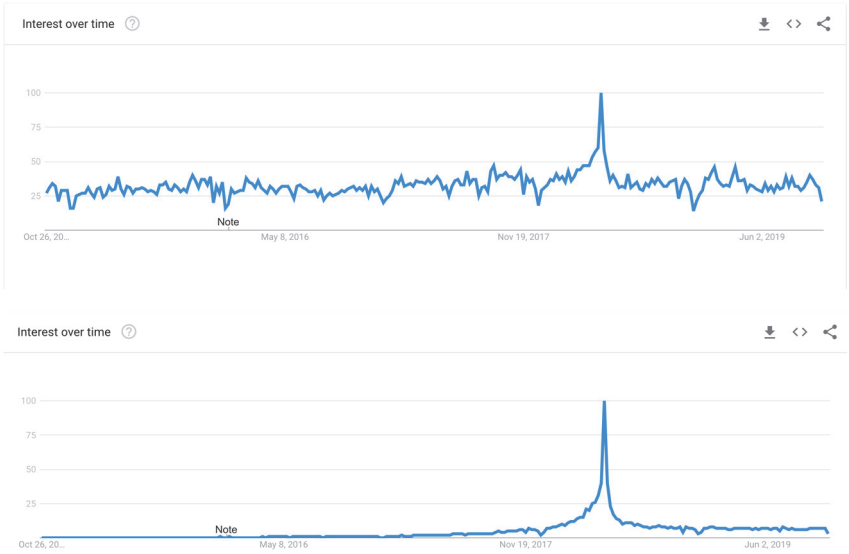
The introduction of the GDPR has certainly focussed minds in terms of data protection. Use of Google search data shows the frequency of searches for both Data Protection and GDPR specifically spiked around the time of the introduction of the regulation and most organisations will have undertaken training of their staff about GDPR, with many new organisational rules introduced as a consequence. Many of us will be familiar with the phenomena of organisational cultures of anxiety regarding data protection in the wake of the introduction of the GDPR, often leading to the imposition of rather overstated restrictions. However, in truth, in relation to the treatment of personal data in research projects, the requirements of pre-existing legislation (e.g. the Data Protection Act 1998) contained many of the same provisions.

However, the GDPR does enhance these requirements, particularly via what is often referred to as 'privacy by design' or 'default'. Article 25(1) of GDPR suggests:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'*

The area of concern here is that of the treatment of personal data. Wherever a researcher has access to, or collects personal data then the provisions of GDPR and the domestic legislation associated with it (in the case of the UK the Data Protection Act 2018) applies – an appropriate legal basis is required and protections should apply to the collection, storage and processing of data. The GDPR also suggests that personal data collection should be minimised.

Figure 1: *Google searches last five years: Data Protection and General Data Protection Regulation*



Source: Google Trends, accessed 23-10-2019

4. Social Research and Personal Data

Most often, in social research, researchers are relatively uninterested in personal data as a component of their analysis. They may be interested in analysing their data according to criteria that might be used to construct personal profiles at the level of the individual such as ethnicity, gender, disability, area of residence and so on, but usually these are as abstract categories rather than as belonging to that specific individual. The specific individual is present in the research as some kind of 'representative' (even if the quantitative requirements for statistical representativeness is invoked in the research method applied) of the broader social group. The focus is on whether or not differences of gender, ethnicity and so on, influence aspects of the analysis rather than on the specific individual.

The exceptions here are two-fold. First where the research follows a longitudinal design to track changes over time with the same participants, usually where a specific group are subject to some form of intervention or where they are involved in large-scale cohort studies. However, longitudinal designs are

relatively rare in social research because they are administratively challenging and expensive to undertake. In most cases, even where change over time is important, this is explored *via* cross-sectional designs where different samples with similar abstract characteristics are used at different points in time. While in longitudinal designs the specific individuals are important, this is not the case in cross-sectional research.

The second exception is in fact accidental; usually where a confluence of abstract categories means that specific individuals are identifiable. This is the case for example when isolating locational (e.g. small areas of residence) and identity (e.g. gender, age or ethnicity). Recognising that area of residence is a strong factor or predictor of deprivation, small area identifiers (e.g. in the UK Super Output Areas derived from post-codes) and the overlap of these with other factors of deprivation such as age or ethnicity means that even though the focus of research may be on abstract categories which predict or result from deprivation, an accidental implication of this is that recognisable individuals are identifiable in the data.

All that said, for the most part researchers are not interested in personal data for their analysis. In most studies research participants – or data subjects – might be anonymised at the point of data collection, at least in regard to the analytical purpose of the research. However, in the main, because of deeply engrained ethical practices, researchers often unintentionally collect personal data as a product of demonstrating consent and ensuring the right to withdraw. In simple terms; there is a trade-off between administrative requirements to demonstrate ethical practice and data protection requirements to ensure that personal data is treated in line with the requirements of the GDPR (and indeed the predecessor legislation). Frequently researchers may be perfectly satisfied with collecting anonymised or pseudonymised data at the point of collection, but unwittingly turn this into personal data because of the requirement to stay within research ethics guidelines – or, more accurately – normal practice, because as we have seen sectoral guidelines and University procedures often stop short of formally requiring written consent.

The foregoing practices come with considerable costs in terms of administration, resources and the data infrastructure required. For example, because personal data has been collected, researchers are under an obligation to undertake elaborate administrative procedures such as replacing names and identifying information in their data with 'Unique Identifiers' and maintaining a separate record of how these Unique Identifiers relate back to specific individuals, so that promises of the right to withdraw can be upheld. In turn, this means storing data on separate parts of data management systems, and using encrypted data recorders and storage devices while 'in field'. They also come with risks attached.

What we know about human behaviour is that individuals with limited time, facing different pressures and the need to prioritise tasks often take shortcuts. The uncomfortable reality is that many researchers will routinely take risks of non-compliance, taking time to apply unique identifiers, forgetting to separate names and other identifying information or carrying data on unprotected or unencrypted hard drives, laptops and data recorders. Recognising the reality of these human frailties in data protection systems is an important step in minimising risks.

However, here GDPR actually provides a means of resolving the tension between engrained research ethics practice and legal data protection requirements, and the associated costs and risks. According to Article 25(2), ensuring 'privacy by default' means:

> *appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.*

5. Conclusion

If data is being collected for the general purpose of research, but the research question being addressed does not require individual personal data, then the 'specific purpose of the processing' in turn does not require personal data. As such, it may well be opportune to use the new world of the GDPR requirements – and the enhanced obligation to seek 'privacy by default' - as a trigger to rethink research ethics. Specifically, universities and sectoral organisations might want to consider whether to place a greater emphasis on alternative methods of gaining consent which do not inadvertently turn research data into 'personal data'.

The essential question to ask is: 'can the data collected be anonymised at the point of collection, so that no personal data is ever stored?'. Clearly there are further trade-offs here. The right to withdraw after the point of data collection is somewhat compromised here – but providing participants with a unique identifier on their 'information sheet' and only recording this with the data collected in the first place provides a simple mechanism to maintain this.

It also introduces a risk that researchers may not seek consent, or that administrative structures do not trust researchers when recording consent without a 'signature' from a research participant. But here Universities and other research organisations need to consider whether it is more likely that researchers will not

comply with the relatively easy step of ensuring consent – a practice that is deeply engrained in behavioural norms – or that they may take short-cuts in time-consuming data protection practices where they do collect personal data. For the most part, it may well be that unsigned but uniquely numbered unsigned informed consent forms without any record of personal data be sufficient for ensuring administrative requirements while minimising personal data collection from the outset.

HARD LAW AND SOFT LAW ON DATA PROTECTION: WHAT A DPO SHOULD KNOW TO BETTER PERFORM HIS OR HER TASKS

Maria Cristina Gaeta

Abstract

The paper aims to describe the sources of law needed to solve issues in data protection, with particular regard to DPO tasks. In order to elaborate this work, two preliminary steps have been carried out. The first one is focused on the critical analysis of the European and Italian law in the field of data protection. The sources of law include both hard law and soft law, with particular regard, for the second one, to the code of conduct. The second step is to define the relevant topics for DPOs, which are the matters that a DPO has to know to better perform his or her tasks in compliance with the GDPR, explaining the reasons underlying their selection.

Keyword: Data Protection Officer; GDPR; Code of conduct.

1. Introduction

This paper has been prepared as part of the deliverables for the EU-funded project entitled "Training Activities to Implement the Data Protection Reform" (TAtoDPR),[1] EU project aimed at training of data protection officers (DPOs), especially in specific sector which will be better illustrate below (*see* table 1), in their new duties under the General Data Protection Regulation (Regulation

[1] More precisely the TAtoDPR has ben co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020) under Grant Agreement n. 769191. For more information on the TAtoDPR project see: https://www.tatodpr.eu.

2016/679, well known as GDPR).[2] The project has been carried out under the guidance of University of Naples Suor Orsola Benincasa (coordinator of the project) and involved different European countries: besides Italy also the United Kingdom and Spain.[3]

As a matter of fact, GDPR is applicable since May 25th 2018,[4] replacing the Data Protection Directive (Directive 95/46/EC). The data protection regulation was adopted in response to the maximum extension of the processing of personal data and to the development of ever more pervasive technologies, strengthening the main EU data protection regime to the point to entail a real reform on data protection. GDPR brings many changes in terms of much greater harmonisation and cross-border enforcement cooperation between national Data Protection Authorities (DPAs) and the European Data Protection Supervisors (EDPS),[5] also thought the European Data Protection Board (EDPB), established

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1571686089135&from=IT. T

[3] Four Universities and an enterprise are involved in this European project, providing different perspectives and expertise:

Università degli Studi Suor Orsola Benincasa of Naples (UNISOB), is the Coordinator of the project TAtoDPR, with its outstanding tradition in the field of Law and New Technologies, and especially the Interdepartmental Research Centre 'Scienza Nuova' and its 'UTOPIA Lab' and the Research Centre of European Private Law (ReCEPL) both established at UNISOB, specifically dedicated to creating a bridge between social sciences and the realm of advanced scientific and technological development. UNISOB Legal team has already obtained several recognitions for its research activity in the field of data protection.

Universidad de Sevilla (USE) provides an expert team including lecturers and researchers in the fields of Civil Law, Privacy Law, Digital Law and Computer Engineering, providing diverse skills and know-how.

Loughborough University (LBORO), and more specifically the Loughborough Design School, is committed to the study of Cognitive and Behavioural aspects of data protection.

University of Derby (DER) contributes with a strong interest and competence in the fields of Law and Political Economy applied to the domain of Data Protection.

RE:Lab s.r.l. (REL) brings long-standing interest and experience in the field of HMI (Human-Machine Interface), including computers, smartphones and other devices, as well as in the relationship between individuals, technology and personal data.

[4] Even though, as a rule, the EU regulations come into force twenty days following the publication in the Official Journal of the European Union (OJ), under art 99 GDPR, the Regulation has been applicable after two years from the publication. It means that GDPR was effectively applied from May 25th 2018, but each single EU Member states needed different timeframes for the application of the GDPR in its legal system which depended on the type of regulatory modification to be put in place and this, sometimes, involved the application of the GDPR after the deadline set by art 99 GDPR.

[5] *See* the official website of the European Data Protection Supervisor (EDPS): https://edps.europa.eu. Currently, art 51 and ff. GDPR provides general DPAs' rules.

by the GDPR and which replaced WP29.[6] At the same time, data protection reform introduces new principles on data protection and introduces the new role of data protection officers (DPOs). The DPO also has the task of cooperating with the national or European data protection authorities and act as a contact point for the DPAs for matters related to the processing of personal data (article 39 GDPR).[7]

This paper attempt to briefly analyse the existing data protection regulation (hard law and soft law) in Europe and in Italy, as well as to identify what a DPO should know to better perform his or her tasks in compliance with the GDPR.

2. The sources of law on data protection with particular regard to the difference between codes of conduct and common guidelines

At the European level, as already explained, GDPR replaced the Data Protection Directive of 1995. The data protection reform was a consequence of the exponential increase in data processing also due to the development of ever more pervasive technologies.

The GDPR is a regulation and not a directive, so it is directly applicable in the legal systems of the EU Member States, without having to be transposed into national law, as is the case of the EU directives, included the Data Protection Directive, which bound the Member States only to the end to be achieved but not even to the means to achieve it. The choice for the regulation instead of the directive was well thought out by the European legislator since with the Data Protection Directive a different implementation had occurred at the national level, which resulted in a non-homogeneity of the protections. Contrariwise, the EU data protection regulation has strong harmonizing power. Indeed, although the GDPR has been applicable for just over a year, the national regulatory disciplines of the individual member states already seem more harmonized.

About the territorial scope of the legislation (articles 3-5, GDPR), reference is no longer made to the placement of the terminal into a Member State of the European Union but to the offer of services in EU countries. Therefore, the

[6] *See* the official website of the European Data Protection Board (EDPB): https://edpb.europa.eu. EDPB is regulated under art 68 and ff., GDPR.

[7] The DPO acts as a contact point in order to facilitate the access by the relevant DPA to the documents and information for the performance of the DPAs' tasks or power, respectively mentioned in artt. 57 and 58 GDPR. In particular, the DPO is bound by secrecy/confidentiality concerning the performance of his or her tasks, in accordance with EU or national law (Art 38, par. 5, GDPR). Nonetheless, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and advising DPAs (art. 39, par. 1, let e)).

GDPR is fully applied to companies located outside the European Union that offer services or products to data subjects in the territory of the European Union. Outside the European area, however, there is the general principle of the limitation of the circulation of personal data (purpose limitation and storage limitation) based on the conformity assessment of the guaranteed measures. Compliance with specific procedures and compliance with the data adequacy principle for the non-EU transfer of personal data is required or, failing this, is needed the explicit consent of the data subject or other particular conditions. [8]

Currently, the GDPR is the main hard law existing in Europe for the protection of personal data. However, there are many legislative initiatives to further implement data protection as, for example, the Proposal for an ePrivacy Regulation of 2017, which is a proposal for greater regulation of electronic communications within the European Union, to increase privacy for individuals and entities. More precisely, today the electronic communications are regulated under Directive 2002/58/EC on electronic communications (well known as ePrivacy Directive). Anyways, the directive seemed to not have a strong impact on data protection issues related to electronic communication, including automated processing issue. For this reason, the European Commission carried out an *ex post* Regulatory Fitness and Performance Programme ("REFIT evaluation") of the ePrivacy Directive and verified that the Directive has not guaranteed effective legal protection of privacy in the electronic communication, taking in to account the digital era in which we live. In particular, the REFIT evaluation shows how important technological and economic developments took place in the market since the last revision of the ePrivacy Directive in 2009. Consumers and businesses increasingly rely on new Internet-based services enabling inter-personal communications (e.g. Voice over IP, instant messaging and web-based e-mail services) which fall down the name of Over-The-Top communications services (OTTs). Generally, the OTTs are not subject to the current EU electronic communications framework which has not kept up with technological developments, resulting in a lack of protection of electronic communications. [9] At the end of the REFIT evaluation, indeed, on 2017 it has been published a Proposal for a

[8] The consent to the processing of personal data plays a central role in the GDPR, which specifies that the con sent must be freely given, specific, informed and unambiguous must consist of an express or explicit action signifies agreement to the processing of his or her personal data (art. 4, n.11, GDPR). Furthermore, the consent represents one of the lawful bases for the processing of personal data (Article 6, para 1, let a), GDPR) and of special categories of personal data (Article 9, para 2, let a), GDPR).

[9] Explanatory memorandum of Proposal for a Regulation of the European Parliament and of the Council, of 10 January 201,7 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM(2017) 10 final), 5.

Regulation on privacy and electronic communications (known as ePrivacy Regulation or ePR), which takes into account of the technological development of our society. [10]

In Italy, the transposition of the GDPR was operated by legislative decree no. 101/2018, [11] which led to significant changes to the Italian privacy code in force (legislative decree no. 196/2003) [12] that was compliant with the Data Protection Directive of 1995. The subsidiarity of the reformed Italian privacy code is evident already from the title of the code as amended, as well as, from the first articles, which show how the text contains provisions for the compliance of the national legislation to the provisions of the GDPR (art. 2 Italian privacy code). [13]

One of the main changes introduced by amendment decree is certainly that relating to minors. In particular, the age for expressing consent to data processing within the information society services is set at 14 years (article 2 *quinquies*, Italian privacy code), using the derogation provided by the GDPR which provides for a limit of 16 years reducible up to 13 (article 8, paragraph 2, GDPR). [14]

Regarding, the data protection in healthcare, the new Italian rule (art 2 *septies*, Italian privacy code) provides that the processing of personal data for the purpose of health protection is regulated under article 9 of the GDPR. The article establishes a general prohibition on the processing of special categories of personal data, except in specific hypotheses provided for by the same article. [15] The previous rule of the Italian privacy code authorised the processing of this particular type of data to the consent of the data subject and to the authorisation of the Italian DPA. The new legislation simplifies the situation by no longer providing for the authorisation of the Italian DPA. On the other hand, however, it requires enhanced data protection, introducing the possibility that the Italian

[10] Proposal for a Regulation of the European Parliament and of the Council, of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM(2017) 10 final).

[11] Provisions for the compliance of national legislation with GDPR, d.lgs. 10 August 2018 no. 101, OJ 205, available at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

[12] Italian Data protection code, d.lgs. 30 June 2003 n 196, OJ 174, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678.

[13] Actually, the reformed Code is not only the compliance of national rules to European ones but also contains provisions that are not linked to the European regulation and states something more (eg. for the penalties).

[14] To in-depth the topic of data protection of minors in the digital environment, focusing on the issue of privacy digital consent given by a minor, *see* IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (1) 2018 Familia (online), 1 ff.

[15] See in particular art. 9, par.2, let. H) and i).

Data Protection Authority imposes specific guarantee measures for the treatment of health data (with a revised provision every two years).

Concerning the new privacy figures, in addition to the DPO, the modified Italian regulation, following the GDPR, allows the data controller or the data processor to designate natural persons for perform specific tasks and functions, related to the processing of personal data. These are not the internal data processors, who were required by the previous version of the Italian privacy code but are person in charge of processing (article 4, no. 10 and articles 29, GDPR).

An anther important news is that the Italian privacy code now provides the *Ente unico nazionale di accreditamento*, which is *Accredia*,[16] as the national accreditation body referred to in article 43, paragraph 1, letter b), GDPR. This statement does not affect the Italian DPA to directly assume the charge of such functions with reference to one or more categories of processing (article 2 *septiesdecies*, Italian privacy code).

Finally, the Italian privacy code provides not only administrative fines (art. 166, Italian privacy code) but also specific penalties for data breach (article 167, Italian privacy code), compared to the provisions of the GDPR that do not expressly provide penalties but only compensation for damages (article 82, GDPR) and administrative fines (articles 83 ff., GDPR). At the same time, however, GDPR, admits the possibility for Member States to establish other penalties (art. 84, GDPR), as well as other administrative fines for the infringements of national rules adopted within the limits of the GDPR (Recital 148) and Italy acted in this light[17].

Coming to soft law, codes of conduct are very important even though, at the moment, in the field of data protection codes of conduct are provided only at the national level. The codes of conduct are rules of conduct or uniform practices in general developed by various international, European or national bodies. They are non-binding provisions (i.e. the codes of conduct are soft law) even if the authority of the body they come from ensures that they are widely applied. The codes of conduct are tools of self-discipline that allow representatives and trade associations to define international, European or national rules to create uniformity within a specific sector (eg. data protection). This self-discipline rules should not be

[16] Accredia is a recognized association which operates on a non-profit basis, under the vigilance of the Italian Ministry of Economic Development. It is the sole national accreditation body appointed by the Italian government in compliance with the application of the GDPR, attesting «the competence, independence and impartiality of certification, inspection and verification bodies, as well as testing and calibration laboratories». For more information see the official website: https://www.accredia.it

[17] At the same time, the initial approach of compliance with the GDPR is rather soft, as expressly stated in art. 22 para 13, d.lgs. no. 101/2018, which foresees that for a period of 8 months the Italian DPA will have to take into account the fact that it is a new law, in the application of fines and penalties.

confused with the guidelines, which are a set of systematically developed information, based on continuously updated and valid knowledge, drawn up in order to make a desired behaviour appropriate and with a high-quality standard. Often, guidelines are produced by multidisciplinary groups and offer a broad definition of good practice. They are contained in documents brought to the attention of a group of interested parties and constitute a starting point for setting up shared behaviours in organizations of all kinds (both private and public) in the social, political, economic, corporate, medical and so on. Nevertheless, as the codes of conduct, the guidelines are soft law because they are not mandatory procedure.

Certainly, the codes of conduct play a very important role in the new data protection system. The GDPR, indeed, foresees the burden of proof, on the data controller (and to the data processor), that has to demonstrate to have implemented the adequate organizational and security measures for the protection of personal data (article 24, GDPR). The codes of conduct, therefore, can be used as evidence in this sense in avoiding high fines; however, the codes of conduct do not guarantee themselves the compliance with the GDPR.

3. An overview of the code of conduct in Europe and in Italy

In the European union, the codes of conduct are fundamental to avoid actions contrary to the GDPR by a specific category of data processor and data controller. This happens both because the codes of conduct contain the description of legal and ethical behaviours considered most appropriate in the reference sector and facilitate compliance with GDPR. In fact, the GDPR attaches great importance to codes of conduct and provides that Member States, Data Protection Authorities (DPAs), the European Data Protection Board (EDPB) and the Commission encourage the development of codes of conduct intended to contribute to the correct application of the GDPR, according to the specific needs of the different kind of the processing and that of micro, small and medium enterprises (art. 40, GDPR). On this point, moreover, the GDPR states that associations and other bodies representing the categories of data controllers or data processors may draw up codes of conduct, amend them or extend them, in order to specify the application of the provisions of the GDPR with particular regard to the topics expressly indicated in the article itself (among many others, for example, are mentioned the collection of personal data, the pseudonymisation, the exercise of the rights of the interested parties, as well as the notification of personal data breaches to DPAs.). [18] Code of conduct represents a way to apply the

[18] Aspects that could be regulated by codes of conduct are the following, as stated in art. 40,

accountability principle which consists in the obligation to assume responsible management that takes into account the risks connected to the activity carried out and that is suitable to guarantee the full compliance of the processing with the principles enshrined in the GDPR and national legislation. The result is the responsibility of the data controller and the data processor who are entrusted with the task of deciding autonomously the methods, the guarantees and the limits of the processing of personal data, also thanks to the adoption of codes of conduct. [19]

The associations and other bodies indicated in GDPR that intend to draw up a code of conduct, amend, or extend an existing one, have to submit the draft code to the DPA which is competent under Article 55 GDPR. The competent DPA expresses an opinion on the compliance with GDPR of the draft code, or the amendment, or the extension, and approves it, if it considers that it offers sufficiently adequate guarantees. If the DPA approves the code of conduct, it has to register the code and publishes it.

In the event that the draft code of conduct refers to the processing activities in different Member States, before approving the draft code, the amendment or the extension, the competent DPA submits it, through the so-called consistency mechanism (art. 63 GDPR), to the EDPB, which formulates an opinion on compliance with the GDPR of the draft code, its amendment or its extension. In the case in which codes of conduct are adhered to by controllers or processors that are not subject to GDPR (*see* article 40, para 3, GDPR), the EDPB have also to verify if there are appropriate safeguards. So far as the EDPB opinion confirms the conformity of the draft code or its amendment or extension, the EDPB will forward its opinion to the Commission. Finally, the Commission can establish that the code, the amendment or the extension has general validity within the EU and

---

para 2, GDPR: « (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79».

[19] In any case, the adoption of codes of conduct is not the only instrument made available to data controllers and data processors in order to comply with the accountability principle. These should in fact be considered together with other important means, such as the DPIA (art. 35, GDPR) and the certifications (art. 42, GDPR).

there the Commission provides adequate publicity for the approved codes with general validity and the EDPB collects all the codes of conduct, amendments and extensions approved in a register and makes them public by appropriate means.

On 12 February 2019, the "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679", [20] which are the first guidelines on codes of conduct, were adopted by the EDPB to promote and encourage the development of these self-regulatory systems, that to date is implemented to a limited extent. The merit of these guidelines is that they shed light on the procedures and rules relating to the presentation, approval and publication of codes of conduct at both national and European level. The guidelines also provide indications on the minimum contents necessary for the codes of conduct to be accepted by the competent DPA.

It is important to underline that the codes of conduct are not new to the Italian legal system. Before the adoption of the GDPR, the Italian privacy code, under article 12, provided the possibility of signing codes of ethics and good conduct (in Italian "codici di deontologia e buona condotta"). The codes of ethics and good conduct approved were deontological rules (in Italian "regole deontologiche") contained in Annex A of the Italian privacy code and the same have recently been reviewed by the Italian DPA and published in the Italian Official Journal (as provided under article 20, para 4, legislative decree no.101 / 2018). Specifically, the updated texts were published in the Italian Official Journal in January 2019 and concern: the processing of personal data in the exercise of journalistic activity, the archiving in the public interest or for historical research, the statistical or scientific research purposes, carrying out defensive investigations or asserting or defending a right in court. [21]

As the facts show, in Italy the codes of conduct are very important and currently the Italian DPA has approved several, defining them deontological rules.

---

[20] The Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 of the EDPB are freely available here: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it.

[21] More precisely currently there are seven Italian codes of conduct attached to the Italian privacy code: A.1. Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica; A.2. Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica; A.3. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale; A.4. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica; A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti; A.6. Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria; A.7. Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale.

Article 2 *quater* of the Italian privacy code requires the Italian DPA to promote the adoption of deontological rules and verify their compliance with current regulations, especially for activities that involve the processing of data necessary for the fulfillment of legal obligations (article 6, paragraph 1 letter c), GDPR), for the execution of a task of public interest or connected to the exercise of public authority (Article 6, paragraph 1, letter e), GDPR) and for data genetic and health related (Article 9, paragraph 4, GDPR).

4. Main data protection topics for DPOs

After analysing the sources of law on data protection and the principal innovations resulting from the data protection reform, this paragraph illustrates the main data protection topics regulated in the abovementioned sources of law that a DPO should know to better perform his of here tasks. Such subjects have been examined to produce a list of topics and sub-topics for training of DPOs. More precisely, it is the result of a study conducted for defining the topics of interest for a DPOs' training course within TAtoDPR project, better illustrated in the table below.

The proposed list of topics has followed the guidelines provided by national DPO Certification Bodies and the national Data Protection Authorities in Spain, in Italy and in the United Kingdom, intending to produce courses which could benefit from certification schemes. [22]

As we will try to demonstrate the data protection reform has embarked on a new march to the already articulated discipline envisaged at European and national level. In fact, to respond to technological developments and new models of economic growth (recital 6, GDPR), the GDPR has provided technologically neutral protection rules, which apply regardless of the technique used and the automation applied (recital 15, GDPR). Furthermore, the GDPR modifies the basic system of the processing of personal data, proper to Directive 95/46/EC and national legislation, about the organizational and business models and the obligations of the data controller and data processor. However, at the same time, the fundamental principles related to the data subjects, and their rights and du-

[22] In particular, the Spanish Data Protection Authority has published the general guidelines that regulate the Certification Scheme for the DPO figure. Spanish Data Protection Authority has published the general guidelines are available at: http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/SCHEME_AEPD_DPD.pdf. The Spanish DPO Certification Body is ANF (www.anf.es). The DPO certification is regulated by the ISO standards and has an international recognition. In Italy, this certificate will be issued in compliance with the regulation UNI 11697:2017.

ties are conserved, even with some modifications.

With the GDPR, administrative obligations have been reduced, despite the reintroduction of obligations to fill documents related to the processing of personal data (eg. Records of processing activities, under articles 30, GDPR). Furthermore, the processing of personal data, which are carried out according to the law, are conducted "at risk" of the data controller and, eventually data processor.

Moreover, the European Regulation does not affect the existing oligopolistic market structure in the field of personal data even though does not hinders the entry of new players (expressly provided by GDPR, as the DPO, or developed in the practise, as the person in charge for the processing) or formally encourages the subdivision of tasks between the existing figures (eg. sub-data processors in the case in which the data processor engages another data processor). In this light, a very important measure introduced for the protection of personal data concerns the appointment of the new control figure represented by the Data Protection Officer (Articles 37 ff., recital 97, GDPR). The DPO is a physical person, who requires a third-party position and acts as a consultant for the data controller or the data processor, in order to ensure correct management in companies and institutions and act as a contact point between the Authorities. The figure of the DPO is mandatory for public subjects, in the case of treatments that require regular and systematic monitoring on a large scale or in the case of special categories of data (pursuant to Article 9, GDPR) or personal data relating to criminal convictions and offences (pursuant to Article 10, GDPR).

The GDPR does not fail to identify a series of preventive measures that the data controller must adopt, even if there are provisions that overturn the duty of data protection on the organization and on technological instruments. In this way, we can consider the Data Protection Impact Assessment, abbreviated as DPIA (recitals 84 ff. and articles 35 ff., GDPR) applicable in case of high risk for data subject's rights and freedoms. Another important preventive measure is the design of systems aimed at minimizing the use of personal data (data protection by design and data protection by default, under article 25, GDPR), which are technical and organizational measures aimed at reducing the risk for personal data (such as pseudonymisation).

The preventive measures listed are intended to make accountable the behaviour of the data controller (accountability principle, under articles 2 and 24, GDPR) concerning the adoption of procedures able to avoid data risks, in order to prevent high administrative fines. On the other hand, the codes of conduct (articles 40 and 41, GDPR) and the certification mechanisms issued by a qualified body or by the data protection authority (article 42 and 43, GDPR)) can be interpreted in the sense of an improvement of the organizational data protection models (article 35 ss., GDPR).

In the same direction of the preventive measures, go the affirmation of data subject's rights stated in the GDPR (the right to be forgotten, under article 17, GDPR and the right to data portability, under article 20, GDPR), as well as, the uniform regulation within the single market of data processing of those who are on the territory of the European Union, guaranteed by the European Data Protection Board (article 68, GDPR), which is in addition to the existing European Data Protection Supervisor and national Data Protection Authorities.

Anyway, for the case in which the *ex ante* protection is not enough, GDPR introduced high administrative fines (articles 83 ff., GDPR), up to 2% or 4% of the annual worldwide turnover of the previous year[23]. The GDPR also provides compensation for damages (article 82, GDPR), but without significant innovations in comparison with the previous regulatory framework (Directive 95/46/EC)[24]. The tightening of administrative sanctions can be interpreted in the sense of increased deterrence. Finally, even if the GDPR does not expressly provide penalties, as already said it admits the possibility for Member States to establish other penalties in case of non-compliance with GDPR (art. 84), as well as other administrative fines for the infringements of national rules adopted within the limits of the GDPR (Recital 148).

---

[23] More precisely, chapter VII of the GDPR regulates Remedies, liability and penalties. In this context, art. 83 GDPR distinguishes two groups of administrative fines: minor fines and major fines. Indeed, it provides minor fines (so to speak) up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year in case of the infringements of the obligation imposed on: (a) the data controller and the data processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43 GDPR; (b) the certification body pursuant to Articles 42 and 43; (c) the monitoring body pursuant to Article 41(4). The same articles impose major administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year in case of the infringements of: «(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)».

[24] Anyways, in Italy, the d.lgs. no. 101/2018, provide the express repeal of the art. 15 of Italian privacy code, which has regulated the right to compensation for data breach. This is the reason why, also in Italy art. 82 of the GDPR is the new fundamental rule on civil liability in the processing of personal data and the consequent right to compensation for damage. Anyways, from an in-depth analysis of the case-law at European and national level, emerged the difficulty of proving the damage coming from the unlawful processing of personal data in the field of civil liability. This study is a work conducted by the Research Center of European Private Law (ReCEPL) at Suor Orsola Benincasa University of Naples, which will be published separately, and it took into account both case law on art. 15 of the Italian privacy code and these on art. 82 of the GDPR.

The above-mentioned regulatory choices reveal an approach aimed not to prevent the increasingly massive production and processing of personal data made by new technology and techniques that allow the multiplication of the data themselves and of their processing, but to regulate the processing with mechanisms which have the purpose of minimizing the risks of loss, dispersion and diffusion of personal data, in order to protect the sphere of the data subjects.

Technology (eg. privacy by design, through anonymisation and pseudo-anonymisation)[25] is called upon to regulate technology according to the objectives set by the European legislator, while the legal rules gain their own important role concerning the sanctions. However, it remains to be seen whether the techno-regulation as well as the careful use of the sanctioning power by the DPAs and the national courts will be efficient, performing the desired *ex ante* and *ex post* protection. This problem derives from the fact that, the GDPR does not have much impact on some incoherent approaches, as in the case of automated processing of personal data, including profiling process, that must be the object of timely information, authorisation, and right of opposition (article 22, GDPR). With regard to user profiling, reference should be made to the regulatory provisions according to article 4, n. 4, recitals 32, 60, 63, 70, 71, 72, articles 13, para. 2, lett. f), 14, para. 2, lett. g), GDPR that, however, do not regulate profiling issue completely and protectively because do not provide specific preventing measures (*ex ante* protection) or specific deterrent measures (*ex post* protection).[26]

[25] Privacy by design together with privacy by default are important novelties introduced by the GDPR (art. 25). These are adequate technical and organizational measures which aim to protect the data from unlawful processing. This implies an innovative conceptual approach that requires data controllers to start a project, providing by design and by default the right tools and settings to protect personal data.

[26] In this already very complex context, with regard to profiling process an important role is played by electronic communications, currently regulated under Directive 2002/58/EC on electronic communications (well known as ePrivacy Directive) as well as the Proposal for an ePrivacy Regulation.

Table 1 - Proposed table of topics that a DPO should know [27]

1. The right to privacy and the right to data protection
1.1 The privacy legislation before GDPR in the countries of the European Union, with particular regard to the Italian legal system.
1.2 Privacy and European data protection law: from Directive 95/46/CE to the new EU Regulation 2016/679
1.3 Codes of conduct and certifications applicable to the processing and protection of personal data
1.4 ISO/IEC technical standards and best practices
2. Privacy Principles
2.1 Lawfulness, fairness and transparency
2.2 Purpose limitation
2.3 Accuracy
2.4 Storage limitation
2.5 Integrity and confidentiality
2.6 Accountability
2.7 Data protection by design and by default
3. The rights of data subjects
3.1 Information to be provided when personal data are collected or not collected from the data subject
3.2 Right to update data
3.3 Right to cancellation (right to be forgotten in relation with press freedom)
3.4 Conditions
3.5 Right to limit the processing
3.6 Right to data portability
3.7 Opposition law

[27] This table has been published in one of the Deliverable of the TAtoDPR Project.

3.8 Right not to be subjected to a decision based solely on automated processing, including profiling
4. Legal provisions on the transfer of personal data abroad
4.1 Binding corporate rules (Bcr)
4.2 Privacy Shield
4.3 Third countries, representatives in EU Member States
5. The consent to the processing of personal data
5.1 Consent provision and demonstration of the provision of consent
5.2 Characteristic and condition of informed consent
5.3 Method of acquiring consent
5.4 Silence, inactivity or pre-selection of boxes
5.5 Withdrawal of consent and preventive information
5.6 Freedom to provide consent
5.7 Minimum elements: indication of the data controller and the purposes of the processing
5.8 Consent of children in the information society
5.9 Specific cases: • Processing and consent to processing in the health sector P • Processing necessary to fulfill a contract • Processing required by law • Processing necessary to safeguard the vital interests of the data subject or other natural person • Processing necessary for public interest
6. Data protection impact assessment (DPIA)
6.1 Setting, structure and dynamic value of the GDPR
6.2 Codes of conduct and impact assessment
6.3 Integration of the GDPR with the D.lgs. 196/2003 on the national data protection
6.4 Integration of the GDPR with the D.lgs. 231/01 on the responsibility of the institutions

6.5 Public interest issues
7. Type of personal data
7.1 Type and classification of data
7.2 Problems related to unstructured data (e. g. data analytics, standard K180) – cyber-attack techniques and countermeasures to avoid them.
7.3 Problems related to the size of data sets (for example, big data)
7.4 Anonymized and pseudonymised data
8. The roles
8.1 Data controller
8.2 Data processor
8.3 Data protection officer (included the professional insurance for DPO and national and international certification)
9. The organisation's processes
9.1 (Automated) Decision-making
9.2 Budget and management structures
9.3 Information strategy
9.4 Monitoring and reporting systems and techniques
9.5 Typical key performance indicators (KPIs)
9.6 Version control tools for the production of K49 documentation - skills development methods
9.7 Specific fields • Banking sector • Labour Law • Public administration • Police justice and security • Health system
10. Critical risks for safety management
10.1 Possible security threats

10.2 The impact of legal requirements on information security
10.3 Company security management policy and its implications for customer, supplier and sub- contractor commitments
11. New emerging technologies and privacy
11.1 Distributed systems, Virtualization models, Mobility systems and Data sets
11.2 Internet of things and Big Data
11.3 Cloud computing
1.4 Cookies, web analytics, and other user tracking technologies
11.5 Cyber security
11.6 Bioethics and biological data
12. Responsibilities , Remedies and Penalties
12.1 The possible threats to the protection of personal data
12.1 The possible threats to the protection of personal data
12.3 Liabilities
12.4 Remedies: the claim to a supervisory authority
12.5 Penalties

5. Conclusions

Data are acquiring a huge role in our society and, in some contexts, they are considered a new currency of exchange. Through the development of new technologies, both the production of personal data and the processing of personal data is massively increasing. This brought two major implications. From one side, data are in the condition to shape our lives and in general to handle new way to perform both public services and business. For instance, weather forecasts, marketing strategies, impact on public policies, and so on, could have a higher reliability thanks to personal data available and their manipulation within algorithms. From the other side, data have at the same time impact on privacy, as they could give an unexpected and quite detailed portrait, even indirectly, on data subject. In this scenario is born the need of greater protection of personal data, which required the data protection reform implemented through the GDPR, even if some areas of the data processing remain not entirely regulated and, for

this reason (also on the basis of the recent law proposals), it is conceivable that the European legislator will intervene again in the matter.

Currently, to provide a strong *ex ante* protection of personal data, GDPR took the decision, among the others, to introduce in certain kinds of public entities and companies a privacy professional specifically dealing with privacy issues referred to data management: the Data Protection Officer (DPO). This figure is designed by the data controller or the data processor and has to perform specific tasks and functions, related to the processing of personal data regulated under articles 37 and following of the GDPR. The DPO is required to be in a third-party position and acts as a consultant for the data controller or the data processor, ensuring correct management in companies and public entities and act as a contact point between the DPAs. The figure of the DPO is mandatory in different cases so that it is one of the major fields of specialization for professionals since it is a very popular figure in the labour market. This is one of the reasons why it is necessary to provide an accurate preparation for those who intend to take on the DPO role.

The hard and soft law on data protection as well as the list of topics deepened in this paper represent a basis in the increase of DPO training activity. They serve as the main support and working tool for the design and implementation of DPO knowledge. Starting from this point, DPO will be able to develop his consciousness and implement his skills.

DATA BREACH DISCLOSURE DUTIES

Mario Renna

Abstract

The Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data, punctually regulates the data breach phenomenon. In the case of a personal data breach, the role of the controller becomes central, because he shall notify the personal data breach to the supervisory authority and communicate the personal data breach to the data subject.

Data breach regulations allow us to appreciate the principle of accountability, the centrality of the risk-based approach in data processing and the need to ensure effective protection of the rights and freedoms of data subjects.

Key-words: data breach; transparency; supervisory authority.

1. Introduction

The new rules established by the European Regulation 679/2016 (GDPR), regarding the communication obligations following a data breach, constitute an important index to grasp: *i*) the value of the effectiveness of the rights of the data subject and *ii*) the principle of accountability.

The dialogue between the data controller and the supervisory authority, as well as between the controller and the data subject, is not the most advanced expression of a dynamic approach to data security, but they are fundamental tools to ensure a continuous monitoring of the status of personal data.

2. Notification of personal data breach to the supervisory authority

The Art. 33 GDPR represents a fundamental change of pace, aimed at enshrining the security of the processing of personal data as a paramount principle and guiding value of the activity of the controller and of the data processor [see also Art. 5, par. 1, lett. *f*), GDPR] [1]. The security of processing aims to protect, on the one hand, the data subject from any risk of damage to fundamental rights and freedoms and, on the other hand, conforms the processing activity at every stage (Art. 32 GDPR) [2].

The obligation of the controller to notify personal data breach to the supervisory authority materializes the more general 'principle of accountability' [3]; in fact, the controller is obliged to notify, unless it is shown that any risk to the rights and freedoms of natural persons is unlikely. It is, therefore, a flexible duty, based on the procedural nature of risk management and modulated in relation to the nature and gravity of the personal data breach, as well as, specifically, the types of risk for the data subject [4]. According to the European Regulation, data breach means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Art. 4, no. 12, GDPR). Therefore, in the event of a breach, notification to the supervisory authority is mandatory for the

[1] See G Finocchiaro, 'Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali', in Ead. (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (Zanichelli, 2019), 12-13, 17; V Cuffaro, 'Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale', in Id., R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli, 2019), 19.

[2] S. Sica, 'Verso l'unificazione del diritto europeo alla tutela dei dati personali?' in Id., V. D'Antonio and G.M. Riccio (eds), *La nuova disciplina europea della* privacy (Wolters Kluwer-CEDAM, 2016), 8. See, also, F. Bravo, 'L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi', in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo*, (n 1) 804; A. Mollo, 'Gli obblighi previsti in funzione di protezione dei dati personali', in N. Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR* (Wolters Kluwer-CEDAM, 2019), 256.

[3] A. Mantelero, 'Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva', in G. Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali* (Zanichelli, 2017), 321.; S. Vigliar, 'Data breach e sicurezza informatica', in S. Sica, V. D'Antonio and Riccio (eds), *La nuova disciplina europea della* privacy, (n 2) 245, 254. Cfr., anche, F. Bravo, *Il 'diritto' a trattare dati personali nello svolgimento dell'attività economica* (Wolters Kluwer-CEDAM, 2018), 107; D. Farace, 'Il titolare e il responsabile del trattamento', in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo*, (n 1) 746.

[4] F. Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I (Giappichelli, 2016), 291, footnote 54.

controller within 72 hours from the time of knowledge, unless there are risks to the rights and freedoms of natural persons. The first paragraph of Art. 33 GDPR shows several critical elements [5].

First of all, it may be observed that the timeliness of the notification is closed within 72 hours of the knowledge. In order to comply with the regulatory obligation, the controller should have a technical structure that allows: i) a constant flow of information; ii) the assessment of the nature of the risks. Only through a specific monitoring and reaction procedure is it possible to regularly fulfill the prescribed duty [6]. The duty of adequate security measures to address and limit the risks of personal data breach requires an effective coordination of logistical plans, a context in which the role played by the controller is also inserted. The processor shall inform the controller without undue delay after becoming aware of a personal data breach (Art. 33, par. 2, GDPR): in the silence of the provision, the terms of execution of this duty can be established conventionally [Art. 28, par. 3, lett. *c*), GDPR).

A further issue arises in the case of cross-border infringements, that is to say concerning the interested parties belonging to different Member States. In this case, through a coordination of Articles 55 and 56 GDPR, it can be argued that, where notification to the public authority is mandatory, communication by the data controller must take place with supervisory authority leader, as the supervisory authority of the main or of the single establishment of the data controller.

With regard to infringements occurring in establishments outside the European Union, pursuant to Art. 3, par. 2, and Art. 27 GDPR, it can be noted that the notification must be sent to the national supervisory authority of the Member State in which the representative of the controller is established in the European Union. The transnational dimension of the personal data breach therefore requires an exclusive and timely exchange of views, in order not to exacerbate the formal obligations of the controller and to ensure that the competent authority takes measures to immediately protect the data subject.

Having said this, it is necessary to consider as the first paragraph of Art. 33 GDPR links the notification obligation to the ascertainment of an etiological connection between data breach and risks for the rights and freedoms of natural persons, assigned to the evaluation of the data controller. With respect to an underestimation of events, then denied by the production of damages, and, therefore, before the risk of liability for damages (Art. 82, par. 1, GDPR) and administrative pecuniary sanctions for non-fulfillment of the obligation to notify [Art. 83, par. 4, lett. *a*), GDPR], it is reasonable to assume that the data controller

[5] P. Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer, 2017), 65.

[6] Bravo (n 3) 110; Mantelero, (n 3) 323.

adopts a so-called 'low-threshold notification behavior' [7].

Regarding the substantive profiles of the notification, it should be noted that it is necessary for the controller to communicate at least: the nature of the data, the categories and the approximate number of data subjects, as well as the categories and approximate number of records and contact details of the data protection officer or other contact point to obtain information. Furthermore, is required: a description of the likely consequences of the personal data - thus emphasizing the centrality of the 'risk based approach' - and the measures taken or proposed to be taken to remedy, including, where appropriate, measures to mitigate the possible adverse effects. In addition to the possibility for the controller to provide additional information to the minimum required by the standard, it is possible to proceed through a notification in phases: more precisely 'where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay'. In the event that the controller does not have all the elements normally required for notification, he can carry out the obligation of information in a graduated manner: in this way, the controller fulfils its obligation, justifying the reasons for a non-exhaustive notification, and has an immediate contact with the supervisory authority.Finally, the responsibility of the data controller is linked to the record of any data breach, as well as of the consequences and countermeasures taken for this purpose. This information support must allow enable the control authority to verify compliance with the regulatory provisions.

3. Communication of data breach to the data subject

Following the occurrence of data breach phenomena, the obligation to inform the data subject is left to the assessment of the level of risk carried out by the data controller, possibly assisted, in relation to their mutual skills, by the processor and the data protection officer [8]. In order to prevent arbitrary assessments, *Recital* 76 GDPR indicates that the risk assessment should refer to a concrete and prudent analysis and, at the same time, should be based on objective criteria [9].

---

[7] Voigt and von dem Bussche (n 5) 68.

[8] N Brutti, 'Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer', in E. Tosi (ed.), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy (Giuffrè, 2019), 144.

[9] *Recital* no. 76 'the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk'.

Risk assessment is a fundamental step to demonstrate the adequacy of organizational arrangements in terms of security processing. Unlike a probabilistic assessment (*ex ante*), which is the one conducted in the data protection impact assessment, Art. 34 GDPR invites you to estimate the risk through a precautionary assessment and subsequent to the infringement [10].

The communication to the data subject complements the duty to react and reduce the harmful consequences: this communication must allow the data subject to be aware of the risks and to be able to react promptly and effectively [11]. Furthermore, the GDPR conditions the mandatory nature of notification to the ascertainment of an etiological link between data breach and high risks for the rights and freedoms of natural persons: also in this case, in order to avoid administrative and tortious liability, it is easy to foresee that the data controller adopts the low-threshold notification behavior.

The communication obligation is elastic: it is not required if the controller has implemented adequate technical and organizational protection measures and these measures have been applied to the personal data affected by data breach (in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption).

At the same time, the communication must not work where the controller has immediately implemented measures to prevent the occurrence of a high risk to the rights and freedoms of data subject. In such cases, the communication does not uarantee an effective protection of the person concerned and would involve a mere bureaucratic burden. Furthermore, communication will not be required if it would involve a disproportionate effort. In this case, a public communication or a similar measure is carried out according to which the person concerned is informed equally effectively. The exemption circumstances, in order not to frustrate the effectiveness of the rights of the data subject, must be interpreted in a restrictive and objective manner, taking as a parameter of the non-execution the concrete presence of unforeseeable circumstances, such as to alter the normal course of 'processing'.

With regard to the substantive profiles, it should be noted that the controller is required to: *i*) provide details of the data protection officer or other contact point where more information can be obtained; *ii*) describe the probable consequences of the personal data breach and the measures taken or to be taken to remedy and, furthermore, to mitigate the possible adverse effects [12].

---

[10] A. Mantelero, 'La gestione del rischio', in G. Finocchiaro (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (n 1) 524.

[11] Voigt and von dem Bussche (n 5) 96-97.

[12] See, Pizzetti (n 4) 294.

4. Data breach between responsibility and transparency: WP29 Guidelines Personal data breach notification under Regulation 2016/679

The Guidelines on Personal data breach notification under Regulation 2016/679, as last revised and adopted on 6 February 2018 by the WP29, clarify the operation of the dialogue between the controller, the supervisory authority and the data subject. The Guidelines appear to be very useful in highlighting some points of non-immediate clarity. First of all, the moment of the actual knowledge of a data breach by the controller – starting from which the 72 hours for the notification begin – coincides with the moment in which there is a reasonable awareness of the verification of a security incident that compromise the personal data.

The time factor undergoes obviously variability according to the circumstances of the breach: however, 'the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required' [13].

The time factor is also related to the structural dimension of the security system. The Guidelines show that it is appropriate to have effective and efficient internal procedures, regulated by alert mechanisms and inspired by a fruitful cooperation between the controller, the processor and the data protection officer. The plurality of subjects involved in the processing confirms the need to activate synergistic procedures, functional to the preventive relief of data breach risks and to the adoption of reparatory and restorative measures following damage caused [14].

Therefore, notification to the supervisory authority becomes a dialogue between the controller and the public authority, but also a communication conditioned by the flow of data deriving from the collaboration between the controller, the processor and the data protection officer. Pursuant to Art. 33, par. 2, GDPR, the processor 'shall notify the controller without undue delay after becoming aware of a personal data breach', providing any information useful for the final decision of the controller to notify the data breach or less. Furthermore, the presence of the data protection officer is of fundamental importance if it is deemed to have the duty to inform and advise the controller or processor, and to cooperate with the supervisory authority and act as a contact point with the su-

[13] WP29 Guidelines Personal data breach notification under Regulation 2016/679, 11.

[14] Brutti, (n 8) 143; R Panetta, 'Privacy is not dead: it's hiring!', in Id. (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018* (Giuffrè, 2019), 18.

pervisory authority on any request relating to the data processing (Art. 39, par. 1, GDPR).

The notification obligations intends to guarantee an effective protection of the fundamental rights and freedoms of natural persons: safeguarding these rights and freedoms demonstrates the relational dimension of data processing, but it also constitutes a limit for notification. Indeed, the data controller, having ascertained the nature and the impact of the data breach, may refrain from informing the public authority when it is unlikely to harm the rights and freedoms of natural persons [15]. The risk assessment therefore becomes particularly relevant in order to guide the behavior of the controller [16].

With regard the data breach communication to the data subject (Art. 34 GDPR), the Guidelines reiterate the need to ensure effective protection of the rights and freedoms of the data subject, specifying the boundaries of the communication. First of all, note that the communication must take place without undue delay. The controller, as soon as possible, must inform the data subject, so that he can take the most appropriate measures to protect himself from further negative consequences of the breach. Communication must be effective and rendered in a understandable language; therefore, it cannot be transmitted through generic sources (press releases, company blogs), thus discounting an unjustifiable rate of abstractness, nor, even less, alongside other non-conferring news with the actual phenomena of data breach [17].

---

[15] See, e. g., A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche* (ESI, 2019), 187.

[16] *Recital* no. 75 'the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects'.

[17] The Guidelines precise that 'examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximiz-

As previously stated, the data breach notification (a) and the data breach communication (b) are functional to safeguarding the fundamental rights and freedoms of natural persons, therefore they are not absolute and are calibrated with respect to a risk (a) and the high level of risk (b).

In general, when assessing the risk to individuals due to a violation, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria: a) the type of breach; b) the nature, sensitivity, and volume of personal data; c) ease of identification of individuals; d) severity of consequences for individuals; e) special characteristics of the individual; f) special characteristics of the data controller; g) The number of affected individuals.

5. Concluding remarks

The security of the processing and the effectiveness of the protection of the data subject – guiding principles of the GDPR – find concretization in the duty imposed on the data controller following the data breach. Risk assessment translates the principle of accountability: only a correct risk assessment will allow the data controller to punctually comply with the GDPR discipline and not to be exposed to administrative or extra-contractual liabilities.

Risk assessment also evokes the need for a structured risk management system: it is therefore necessary to have several professional figures involved in data processing and to adopt adequate and effective prevention and reaction measures. The effectiveness of the protection of the rights and freedoms of the data subject is clearly stated in the disclosure duties: it is, therefore, necessary for the data subject to be informed of the extent and consequences of the data breach. Only through a continuous knowledge of the state of one's personal data are the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data really protected (Art. 1, par. 2, GDPR).

es the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel'.

MINORS AND NEW TECHNOLOGIES: FROM PARENTAL RESPONSIBILITY TO PARENTAL CONTROL IN BALANCING WITH THE CHILD'S RIGHT TO PERSONALITY

Livia Aulino

Abstract

This article deepens the relationship between minors and new technologies. The legislation of reference is preliminarily represented by the main international charts on the protection of minors, to which are added the most recent rules on the data protection as well as the rules of the civil code. In particular, it is examined the issue of parental control and whether this technological control falls within the broader concept of parental responsibility and in the parental supervision obligation sanctioned by article 2048 of the Civil Code. At the same time, it is examined the right to the online personality of the child, which emerges even more in the current historical context, in which the age of Internet access is always lower and lower. This is also seen in the light of the recent European regulation on the data protection which has recognized the consent given by a child of at least 16 years. Finally, it is dealt the system of negotiation deeds concluded by the child with through the use of the technological tool.

Keyword: privacy law, minors, data protection, new technologies, consent, online negotiation deeds

1. Legal aspects of parental control

Currently the protection of the child manifests itself through an educational control of the parents towards their children, an expression of parental responsibility [1],

[1] The notion of parental responsibility has replaced that of 'parental authority', and was intro-

to which, following the development of new technologies, a technological control [2] has been added, the so-called parental control, which parents can predefine on all operating systems of computer devices used by the child. Parental control is the system that allows the parent to monitor or block access to certain computer activities to the child, which can be dangerous for him, and also to set the maximum duration of use of the IT device.

The parental control can be applied to any device on all common operating systems, such as Windows, Android [3], Apple [4] e Linux, on telephone lines [5], on videogames and up to the most used search engines [6].

All this is relevant also from the legal point of view, where currently, there is no specific regulatory provision, nor jurisprudential precedents that can regulate these issues [7]. Yet, it is believed that the obligation to control access to the internet on time and in the content may fall within the broader concept of parental responsibility. In fact, the obligation to supervise parents against their children in the use of technology, in particular the Internet, can be inferred from the

---

duced by Legislative Decree 154/2013 which rewrote the articles 315 and seq. of the civil code. On the one hand it has better identified the duties of parents towards their children, and on the other it has pointed out the duties of children towards their parents. Parental responsibility exists in all cases where there are children, regardless of whether they were born within or outside marriage.

Currently, therefore, the reciprocal rights and duties of children and parents are regulated in two different peers of the civil code, that is by articles 315 and 337 *octies* of the civil code, and by articles 143 to 148 of civil code, which sanction the rights and duties that arise from marriage, among which those towards children stand out. C.M. Bianca, *Diritto civile, La famiglia*, 2.1, (6th edn., Giuffrè, 2017), 377,380.

[2] Certainly communicating with children, helping them to understand what can happen using the web in a distorted way, giving them limitations and clear information, is the best way to prevent any risk. Often, however, a communicative prevention cannot suffice to defend the little ones from the web's pitfalls, and therefore the parents choose to resort to a digital control to monitor the online behavior of their children limiting their access

[3] In Android, an app has been designed that allows parents to approve and block their child's smartphone apps, as well as to block calls, sending messages or performing activities that could cost money. Among the Premium features (for a fee) there is the possibility of setting a timer to limit the daily use of the device and a timer to block the operation of the app after a specific period of time.

[4] In Windows, Mac OS X, Android, iOS, Kindle, Nook exists the free qustodio app that allows you to have a glance on your child's social and non-social activities. It can block unwanted sites, defend against cyber-predators and cyber-bullies, control phone calls and geolocate the child.

[5] Telecom, Tim, Wind and Vodafone Junior provide for the installation of the parental control.

[6] Search engines such as Google, Safe, Search include parental control installation.

[7] On the subject see F. D'Ambrogio, 'Parental control: accorgimenti tecnici per escludere da parte dei minori la normale fruizione di contenuti classificati a visione non libera', in L. Gatt, *Il diritto di famiglia nell'era digitale*, (Pacini, 2019).

reading in conjunction with the provisions of Articles 147, 316 and 2048 of the Italian civil code, and the jurisprudential guidelines on the duty of supervision of minor children at the expense of parents.

The jurisprudential guidelines according to which the parent to be exempt from civil liability for not having fulfilled the supervision obligation of the minor child, pursuant to article 2048 of the Italian civil code, must demonstrate both that they have given a correct education to their child, but also that they have been adequately supervised. Even it would be appropriate to impose on parents the use of parental filters that can contain the dangers related to the free movement of minors on the internet, in compliance with the obligation of supervision under art 2048 Italian civil code.

On this point, an important jurisprudential case of the Court of Teramo [8] reaffirmed the need for a monitoring activity on the part of parents on their children, and more precisely stated that to be exempt from liability pursuant to article 2048 of the Italian civil code, must positively demonstrate that they have fulfilled the educational burden by indicating to the offspring rules, knowledge and forms of behavior as well as providing the indispensable tools for the construction of truly meaningful human relationships for the best realization of their personality, but also to have then effectively and concretely checked that the children have assimilated the education imparted to them, with the consequence that the gravity and the repetition of the behaviors put in place can then be index of the degree of implementation of such a work of verification.

Even more recently, the Court of Rieti with judgement no. 312/2019 stated that, in the event of damage caused by the minor, the parents must prove that they have given their child an appropriate education to their social and family conditions, as well as having exercised age-appropriate supervision and aimed at correcting non-behaviors correct, in compliance with article 147 of Italian civil code. If this release evidence is not provided, it would be applied the article 2048 of the Italian civil code.

2. The balance between parental responsibility and the right to the personality of the child

At the same time the question aires if is legitimate for a parent to control the minor child in the use of the Internet by operating a stable interference in his privacy.

[8] The case of the Court of Teramo of 02/16/2012 is commented in: I. Famularo, 'La responsabilità genitoriale per mancato controllo dei figli su Facebook', in M. Bianca, A. Gambino, R. Messinetti, *Libertà di manifestazione del pensiero e diritti fondamentali. Profili applicativi nei social network,* (Giuffrè, 2016), 207 and seq.

On the one hand, the parents have the obligation of parental responsibility and therefore to protect their children from phenomena such as pedophilia, grooming [9], cyberstalking. On the other hand, parents should also respect the child's personality and the freedoms recognized to them, both at constitutional and international level.

In this regard, article 16 of the 1989 New York Convention protects the child's privacy; the same Convention, in article 17, recognizes the importance of the function exercised by the mass media and the States "*ensure that the child has access to information and materials, especially if aimed at promoting his social, spiritual and moral well-being and his physical and mental health*".

Therefore, it is considered legitimate a power of control over one's child understood as the right to monitor the use of the technologies by the minor, but with a reasonable measure proportionally also at the age of the same; this in order to prevent the supervision of parents on online minors from becoming cyber-stalking.

3. The digital consent of children online

The need to guarantee the right to the child's online personality emerges even more in the current historical context, in which one is always connected, and in which the age of Internet access is always lower. The European regulation 2016/679 [10] has introduced a specific discipline for the protection of the data of the minors, whose defense turns out to be strengthened and differentiated. This is a new law as the previous EC Directive 46/1995, on data protection, did not include any specific provision on the age of minors [11]. At the same time, Legislative Decree no. 196/2003 (so-called Italian privacy code), of application of the mother directive in our legal system, provided that the consent of a minor

[9] In Italian law the "*grooming*" crime was introduced with Law n. 172/2012 and is governed by article 609 - undicies of the penal code; it punishes "*any act aimed at obtaining the trust of the child through artifices, flattery or threats also put in place through the use of the Internet or other networks or media*". Sul punto vedi: I. Salvadori, *L' adescamento di minori. Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, (Giappichelli, 2018); L Aulino, 'Sharenting: la tutela del minore online nell'era dei social network', in L. Gatt, *Il diritto di famiglia nell'era digitale*, (Pacini, 2019).

[10] The General Regulation 2016/679 of 24 May 2016, from now on GDPR (General Data Protection Regulation), is the European legislation on privacy and personal data protection. It was published in the European Official Journal on 4 May 2016, and entered into force on 24 May 2016, but its implementation took place from 25 May 2018. Its main purpose was to harmonize the regulation on the protection of personal data to within the European Union.

[11] Directive 1995/46/EC and the privacy code were designed before the Internet transformed the way of life; currently, in fact, children's lives are always online.

was to be delegated to the legal representative, being unable to act until he reached the age of majority [12].

The recent Regulation, in several points, draws attention to the protection of children's personal data, reversing the orientation of the previous legislative texts on the subject [13]. Indeed, the point 38 specifies that "*children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child".* Also the point 58 specifies that: "*given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*", a rule that is also included in article 12 of the European Regulation which states that: "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child […]*".

Furthermore in article 6 [14] of GDPR, lett. f), which governs the conditions of

---

[12] This provision was in contrast with the highly personal nature of the right to privacy; moreover, the internationalist conception of the child on an international level (see the New York Convention on the rights of children and that of Strasbourg on the exercise of the rights of children) was not of a subject incapable of acting outright, but of active participation in events of life that concerned him, without the necessary intermediation of the parents.

[13] On the point see IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (2018) 1 *Familia*, 3,23.

[14] Article 6 of the GDPR on the lawfulness of the processing, states that: "1. *Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data sub-*

lawfulness of the processing, the protection of minors acts as a limit to the owner's interest.

The main rule is contained in article 8 of the GDPR [15] which states that in the context of offering information society services aimed at minors, the processing of personal data is lawful if the child who consents is at least 16 years old, but the Member States may establish a younger age, provided it is not less than 13 years old. If, on the other hand, the minor is under the age of 16, the treatment is considered lawful only if the consent is given or authorized by the holder of parental responsibility [16].

The choice of the European legislator is dictated by the circumstance that the relationship that the user establishes with the information society is not limited to the mere registration but takes the form of a real profiling; this implies that the information relating to the user is stored and combined together, giving rise to significant repercussions that can also affect the future life of the child. Therefore, since minors are less aware of the risks and consequences related to their behavior, they need greater protection.

In this regard, the Italian legislator, with Legislative Decree n. 101/2018 of adaptation to the GDPR, set the limit of the "digital age" at 14 years. Other countries have also used the derogation, setting the limit at 14 years (Austria and Lithuania) or at 15 (Czech Republic, Slovenia, France) or at 13 years (Spain, Sweden, Denmark, Estonia, Latvia, Finland, Portugal).

According to some, the choice of the European legislator to prevent autonomous access to digital services to children under the age of 16 appeared to be too restrictive. This is because scientific research [17] has shown that, from the age of 13,

---

ject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks".

[15] **Article 8 on the conditions applicable to the consent of children in relation to information society services provides that: "***1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. 2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child".

[16] L. Aulino, 'Il consenso digitale dei minori su facebook', (2018) *Data Protection Law*, in *http://www.dataprotectionlaw.it*.

[17] A study conducted by the pediatric center Stanford Children's Health has shown that between 12 and 18 the adolescence manifests itself with the development of the cd. complex think-

the child forms his own capacity for discernment; this capacity is also referred to by the Convention on the rights of children and adolescents. Therefore, the immediate consequence for under-16 Europeans (or under 14 Italians), where they have shared sensitive information online, is to choose whether to remove this information or to preserve its publication, with the necessary consent of the parents [18].

4. Negotiation deeds concluded online by the chid

Another problem that may emerge concerns the regime of the negotiating acts concluded by the child, through the use of the technological tool. He, although an easily suggestible subject, whose personality is in formation, however, can make purchases in complete solitude, without the supervision and control of the parents, exposing them to the patrimonial responsibility. The parent, as the legal representative, could in fact be liable, both for the fulfillment of the contractual obligation of the represented person, and for being liable for damages caused by the child following a fraudulent conduct [19].

In the Italian legal system, the principle of non-binding and annulment of the contract (article 1425, 1 co., civil code) applies to the minor, as it is considered a weak consumer due to his or her incapacity subjectivity pursuant to the article 2 of Italian civil code by way of exception, however, the contract concluded by the minor which is useful for the same is considered binding for both parties, satisfying adequately his needs and his personal life conditions.

For other assets, the rule of annulment and binding effectiveness is in any case tempered by the exceptional rule provided by article 1426 of the Italian civil code, according to which the contract cannot be challenged if the incapable person has "*concealed his minor age with deception*". But if he limited himself to claiming to be of age, this is not in itself sufficient to supplement the fraudulent conduct required by the rule for the stability of the contract [20].

---

ing (*http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594*).

[18] Furthermore, since the entry into force of the GDPR, the main social networks, including Facebook, have envisaged that minors should identify, among their contacts or by indicating an e-mail, the adult who exercises parental responsibility, at order to validate their social profile. Consequently, the recipient of the request must comply with the consent to share sensitive data for their child. Yet the child under the age of 18 will be able to remedy the problem by indicating any e-mail address to which he will access and authorize the processing.

[19] On the subject see E. Andreola, 'Il regime degli acquisti on line del minore quale consumatore debole', in L. Gatt, *Il diritto di famiglia nell'era digitale*, (Pacini, 2019).

[20] On the point see F. Messineo, '*Annullabilità e annullamento'*, in *Enc. dir.*, II, (1958) 476, according to which the scam must consist of an "efficient plot" similar to the provision of articles 1439, first paragraph, c.c.

These general rules on the pathology of the contract are also applied in the case of the online store, since the cause, the object and the content of the contracts are identical.

It is instead necessary to clarify whether the specificity of telematic bargaining can have consequences on the rules of consensus building.

In the bargaining system c.d. point and click, by pressing the "*confirm order*" or "*purchase*" button in which a declaration is missing, a problem arises in identifying the subject to which the manifestation of the contractual will must be attributed. If in fact it is easy to go back to the computer from which it was issued, it is more difficult to know the real identity and, a fortiori, the subjective state and the volitional path of the physical person who has used that technology in the transmission operation.

Furthermore it is necessary to distinguish at least three hypotheses: the first includes the cases in which the minor completes the form for the purchase, indicating the real date of birth and payment on delivery, or when the minor does not fill in any form but simply answers affirmatively to the seller's question about the age. In these cases the contract is voidable.

The second hypothesis is that in which the minor indicates a false date of birth in the form to appear an adult, indicating a payment method different from the credit card. The contract is valid (pursuant to article 1426, first part, of Italian civil code). The third hypothesis is that in which the minor is silent about age because the e-commerce site does not require any registration. In this instance the contract is voidable. Recently the case of a two-year-old girl who, playing with her mother's smartphone, unknowingly bought a three-seater sofa on Amazon costing almost $ 400 [21].

In this context, there are article 8 of the European regulation n. 2016/679 and article 2 *quinquies* of the new privacy code [22], that oblige the online service seller to verify, or to have done everything possible to verify, that the consumer is over 14 years old (in Italy) or 16 years (in Europe). Furthermore, the article 8, paragraph 3, specifies that the GDPR does not prejudice the general provisions of the law of contracts of the Member States, such as the rules on the validity, formation or effectiveness of a contract with respect to a minor.

---

[21] The case happened in California to Isabel McNeil, who discovered the purchase made by her daughter only a few days after the transaction, through a delivery notification by the courier. The mother both tried to cancel the order, which had already been sent, and to return the sofa, so she would have to pay about 150 euros for shipping costs. So he tried to resell it on an online trading platform. The matter was easily resolved, when Amazon, having learned of the incident, then offered her a full refund and gave her the opportunity to hold the sofa. *https://www.ilfattoquotidiano.it/2019/10/12/da-il-cellulare-alla-figlia-di-due-anni-per-giocare-lei-compra-un-divano-su-amazon/5511361/ Dà il cellulare alla figlia di due anni per giocare: lei compra un divano su Amazon.*

[22] Legislative Decree no. 196/2003 updated to the Legislative Decree n. 101/2018.

THE IMPACT OF E-HEALTH ON PRIVACY AND FUNDAMENTAL RIGHTS: FROM CONFIDENTIALITY TO DATA PROTECTION REGULATION

Francesco Cirillo

Abstract

This paper aims to address some of the relevant issues of health and privacy within e-health landscape. Scientific progress is actively developing pervasive processing of health data. Once considered as the protection of private life, in the last decades, the concept of privacy has evolved. The main feature is the protection of the flow of personal information in the digital world. The GDPR has introduced a new approach that also entrusts some soft law instruments. The principle of consent has now a different and weaker role. Data-sharing, scientific research, healthcare, privacy and research are placed in a stronger interconnection. In this new framework, deontology and private self-regulation are the ultimate warranty of the balance between health and privacy. Then, the scientific community is entrusted to discover its limits and to be the guardian of a problematic balance between values increasingly transfigured by the disruptive innovation.

Key-words: Privacy, health, e-health, medicine, informed consent, GDPR, scientific research, big data, deep learning, deontology, confidentiality, code of conduct, deliverables, fundamental rights, constitutional law.

Introduction

The purpose of this paper is to address some issues of the relationship between health and privacy, as fundamental rights, in the e-health landscape. [1]

[1] B. Shen (ed.), *Healthcare and Big Data Management* (Springer 2017); C Granja, W Janssen,

New technologies, such as biotech, neurotech and nanotech, have introduced new possibilities in the field of healthcare. [2] The therapy, as a consequence, is no longer limited to removing the disease, but it is extended to the enhancement of human conditions (for example, cosmetic surgery or anti-ageing treatments). The new perspective is well described as a transition from *restitutio ad integrum* to *trasformatio ad optimum.* This new approach to medicine is not limited to the areas of medical intervention, but also includes the use of big data and artificial intelligence in healthcare. [3]

In the empirical model of modern medicine, data collection and data sharing were fundamental activities for scientific progress, and they always involved several risks for privacy and other fundamental rights. [4] The strong connection between scientific progress and processing of health data has now a new role in the context of e-health and big data. Scientific progress is strongly entrusted to innovative and pervasive forms of health data processing. The digitization of health records and some new health care devices have introduced significant changes by using artificial intelligence and data science. [5] Furthermore, in few years we may be connected to an e-health software, which will record our data, concerning health and other personal conditions (e.g. genetic data, consumer life-style data, etc.). Such an e-health system will predict our risks thanks to a general analysis, based on data of other people and then personalized by profiling or by other forms of automated use of data. [6] Likewise, it could analyze and notify for every kind of imperfection with our health, reducing people to a condition that is always pathological and always in need of therapy.

In parallel to healthcare, also privacy is changed: if once it was described just as 'the right to be let alone' [7] (i.e. the safeguard of a private area), in the 'in-

---

MA Johansen, 'Factors Determining the Success and Failure of eHealth Interventions: Systematic Review of the Literature' (2018) 5 J Med Int Res e10235; see also WW Lowrance, *Privacy, Confidentiality, and Health Research* (Cambridge University Press 2012).

[2] R.T. Anderson, C. Tollefsen, 'Biotech Enhancement and Natural Law' (2008) 20 The New Atlantis 79.

[3] N. Mehta, A. Pandit, 'Concurrence of Big Data Analytics and Healthcare: A Systematic Review' (2018) 114 Intern J Med Inform 57.

[4] On the history of modern medicine, EH Ackerknecht, *A Short History of Medicine* (first ed. 1955, John Hopkins University Press 2016); for legal aspects and risks for fundamental rights, H Kupwade Patil, R Seshadri, *Big Data Security and Privacy Issues in Healthcare* (2014) IEEE International Congress on Big Data, Anchorage, AK, 762.

[5] L. Dennison, L. Morrison, G. Conway, L. Yardley, 'Opportunities and Challenges for Smartphone Applications in Supporting Health Behavior Change' (2013) 15(4) J Med Int Res e86.

[6] About the future landscape of e-health, YN Harari, *21 Lessons for the 21st Century* (Random House 2018) Part 1.3.

[7] S.D. Warren, L.D. Brandeis, *The Right to Privacy* (1890) 4 Harv Law Rev 193.

formation society' the idea of privacy turned into something different. We can now define privacy, more than a protection of intimate space, as the protection of the flow of information in the digital world.[8] The General Data Protection Regulation (EU) 2016/679 (GDPR) has introduced a new approach based on the accountability of the players. The controllers «shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed according to this Regulation» (art. 24 GDPR). The meaning is that the controllers have to prove they have planned the mandatory measures for the protection of individual rights. Nonetheless, it is not possible to decipher what these measures should be just by reading the Regulation. It is necessary to link to other legal instruments, such as soft law, communications and other policy instruments, positions of the EU institutions, etc. The approach refers to a trend that characterizes the relationship between public law and new technologies: the innovation needs increasingly soft law instruments.[9]

In particular, the processing of data for medical purposes (e.g. art. 9 GDPR, letters l and i) involves a joint thinking on the issues of medical law, data protection law, data sharing and legal problems of scientific research. Health, privacy and research are placed in ever growing mutual connection. The potential of e-health technology, as well as other new medical intervention techniques, could refer to the bioethical and philosophical issues of posthumanism, which suggest a radical distortion of concepts like therapy, health or disease.[10]

The deontology and self-regulation of the sectors involving this innovation assume the role of the ultimate guarantor of the delicate balance between health and privacy. As we will show in the conclusions, the legal and scientific community will play the specific role of controller of innovation.

1. The impact of new technologies in medical law and bioethics

The first issue we address is that the idea of healthcare is changing. The

[8] As the German constitutional Court stated in 1983, 1 BvR 209/83, in BVerfGE 65, 1-71; on this topic W. Steinmüller, 'Das informationelle Selbstbestimmungsrecht' (2007) 3 FIfF-Kommunikation 15; referring to the Italian legal culture, the first sign of this change already in S Rodotà, *Elaboratori elettronici e controllo sociale* (Il Mulino 1973).

[9] L.G. Trubek, 'New Governance and Soft Law in Health Care Reform' (2006) 3 Ind Health L Rev 139; in Italy, E Tosi, *High tech law: The digital legal frame in Italy* (Giuffrè 2015); in this review, MC Gaeta, 'Hard Law and Soft Law on Data Protection: What a DPO Should Know to Better Perform His or Her Tasks' (2019) 2 EJPLT.

[10] U. Wiesing, 'The History of Medical Enhancement: From Restitutio ad Integrum to Transformatio ad Optimum?', in B. Gordijn, R Chadwick (eds.), *Medical Enhancement and Posthumanity* (Springer 2008) 9.

change mainly relates to what the perception of health is and what therapy should be. Besides this bioethical issue, the power of the new technologies on humans have a huge fallout on legal concepts and fundamental rights. In the continental legal systems, such as Italy, Spain, France or Germany, every person has a broad spectrum of fundamental rights regarding health, healthcare or bodily integrity. [11]

The Italian constitution is the only one that states a general 'right to health' (art. 32 Italian Constitution), a general principle with several meanings. According to the Italian doctrine, there are two different areas of fundamental rights: the freedom in health, which concerns the right to choose the therapy or, in case, to refuse it; then, the right to healthcare, substantially secured in different ways, in different countries and at different times. This distinction reflects the difference of negative liberty (the absence of obstacles to the free will, a kind of continental version of habeas corpus) and positive liberty (the possibility of acting in such a way as to realize one's fundamental purposes), firstly theorized by Isaiah Berlin [12] and in a certain way supported from our doctrine. The 'right to health', the right to 'bodily integrity' and to healthcare, refers to two different meanings of health concept: one is the state in which we are, no matter if good or bad, the other is the state in which we would like to be, a potential future condition. This statement requires reflection on the meaning of the concept of health, because too often it is taken for granted that the term is clear. The World Health Organization, in its Constitution, states that «health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity», [13] but this is a very broad meaning, not so useful in the legal field. As

[11] In Italian Constitution the bodily integrity is linked to the general clause of human rights protection, (*diritti inviolabili*, art. 2), to personal freedom (art. 13) and freedom in healthcare (art. 32), see D. Morana, *La salute come diritto costituzionale* (Giappichelli 2018); likewise, in Spanish Constitution states the *libertad personal* (art.17) and the *derecho a la protección de la salud* (art. 43); in France, there's a mention of health in the Preamble to the Constitution, and in the Charter for the Enviroment, which states that «chacun a le droit de vivre dans un environnement équilibré et respectueux de la santé» (art. 1); also in D. Tabuteau, B. Mathieu, A. Laude, *Droit de la santé* (Presses Universitaires de France 2018); in Germany the *Recht auf körperliche Unversehrtheit* is stated in art. 2 GG, whereas the medical care is linked to the *allgemeine Gewährleistung* of the Government, P Kirchhof, 'Das Recht auf Gesundheit' (2008) na; in United Kingdom, see also M. Weait, 'The United Kingdom: the Right to Health in the Context of a Nationalized Health Service', in J.M. Zuniga, S.P. Marks, L.O. Gostin (eds.), *Advancing the Human Right to Health* (2013) 209; a general perspective in T Degener, M Decker, 'Das Recht auf Gesundheit', in K Walther, K Römisch (eds.), *Gesundheit inclusive*: *Gesundheitsförderung in der Behindertenarbeit* (Springer 2018) 35.

[12] I. Berlin, *Two Concepts of Liberty* (Clarendon 1958); about this distinction in the Italian doctrine, A Pace, *Problematica delle libertà costituzionali* (Cedam 2003) 95.

[13] World Health Organization, *Constitution of the world health organization* (1946), and the

a matter of fact, if we look at the concept of health used in the courts, we will find a concept of health more like bodily integrity, meant as the specific biological state, often still referred to biostatistical conception of health. [14] It is evident that other meanings of health are assumed to distinguish medical care from other kinds of assistance. However, in case of medical care, the health is always the theoretical state in which patient would be, referring to the technological possibilities and to the historical and cultural context. These considerations make it possible to state that health is a relative concept, as it has been demonstrated by the philosophy of medicine. [15] Furthermore, it is possible to state that health has at least two possible general meanings: health as a condition, and health as a goal, whatever they mean.

In a certain way, we could imagine this difference of meaning also as a progressive change of the point of view. Technological innovation in medicine has completely involved the relation to the human body. If two centuries ago, the highest ambition of medical practices was the simple removal of the pathological element (a sort of *restitutio ad integrum*), the current framework is much more complicated. [16] The medicalization extended to every human activity and the technological possibilities suggest a different idea of 'the role of the doctor'. Therapy is no longer just an activity aimed at restoring a lost condition, but it is also the activity that tries to enhance the human being. In this framework, health is not just the condition in which we are, or our bodily integrity, the bio-statistic normality, "a state of complete physical, mental and social well-being", or something else. Health is also a sort of potential goal, a future condition that legitimizes the use of enhancement practices. [17]

Already in the e-health models that are currently being tested, the connection to a network allows a continuous update to monitor one's health. The use of big

comment of FP Grad, 'The preamble of the constitution of the World Health Organization' (2002) 80 Bulletin of WHO 981.

[14] A common definition of health in Italian courts is "the condition of the average human being", M. Rossetti, *Il danno alla salute* (CEDAM 2017) 126; on the biostatistical theory ant its critique B.M. Kious, 'Boorse's Theory of Disease:(Why) Do Values Matter?' (2018) 43(4) J Med Phil 421; *pro* P.H. Schwartz, 'Reframing the disease debate and defending the biostatistical theory' (2014) 39(6) J Med Phil 572; C Boorse, 'A Second Rebuttal on Health' (2014) 39 J Med Phil 683.

[15] On the relative meaning, against the biostatistical theory, D.J. Guerrero, 'On a naturalist theory of health: a critique' (2010) 41(3) Stud Hist Science 272; recently, again, A. Broadbent, *Philosophy of Medicine* (Oxford University Press 2019).

[16] E.D. Pellegrino 'Biotechnology, Human Enhancement, and the Ends of Medicine' (2004) 10(4) The Center for Bioethics and Human Dignity 1.

[17] On the concept of enhancement, JC Heilinger, *Anthropologie und Ethik des Enhancements* (Walter de Gruyter 2010), 59.

data, risk assessment operations and 'patient-user' profiling could play a decisive role both in disease prevention and in strengthening individual health. In this context, then, the concepts of health and therapy could be transfigured entirely, given that they are already making a partial but significant twist. [18] Furthermore, the historical nature and relativity of the concept of health has already been affirmed on the level of the philosophy of medicine, with ample proof of the groundlessness of many defining approaches of the last century. [19] The naive visions of health as a condition of 'normality' have been widely criticized.

As for the law, courts and legal doctrines are still very much linked to traditional notions of health, but the new technology could overwhelm the current legal framework. A humanity that is always connected with health institutions, also thanks to the Internet of Things, could live in a continuous sharing of the healthcare information, with the consequence of living in a dimension that is always 'pathological' and, therefore, always in need of constant diagnosis and therapy. In such a landscape, diagnosis and treatment would not only be sporadic activities; several technological devices could continuously manage our health, considering consumption, activities, displacements, analysis results, genetic tests, etc. These are not science-fiction considerations if we observe that the leading players in the digital sector, both public and private, are planning more and more investments in artificial intelligence in the health sector. [20] A recent case, finally, confirms this assumption and more than one clue leads us to imagine an upcoming disruptive innovation even in this sector. [21]

2. Confidentiality and data sharing in new healthcare models

In the current medical approach and the future, health treatment involves a necessary activity on the patient's data. Indeed, a part of the health treatment coincides with the processing of health data. If, however, this statement seems to have always characterized the doctor-patient relationship, since therapy necessarily involves the

[18] P.D. Scripko, 'Enhancement's place in medicine' (2010) 36 J Med Ethics 293; from a point of view of neuroscience and neuroethics, B Gordijn, 'Neuroenhancement', in J Clausen, N Levy (eds.), *Handbook of Neuroethics* (Springer 2015) 1169.

[19] A. Broadbent, *Philosophy of Medicine* (Oxford University Press 2018) Part. A Chapt. 4.

[20] On the development of e-health, WJM Stevens et al., 'eHealth Apps Replacing or Complementing Health Care Contacts: Scoping Review on Adverse Effects' (2019) 21(3) J Med Int Res e10736; also P. Guarda '"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation' (2019) 1 BioLaw Journal 359.

[21] D. Blumenthal, 'Why Google's Move into Patient Information Is a Big Deal' (2019) Harv Bus Rev 26.11.2019.

management of data, in the digital environment, a different need for sharing the personal information flow is required. The issue entails, first, that the patient's confidentiality cannot be sufficiently protected only by professional secrecy; an obligation that modernity has borrowed from the Hippocratic tradition.[22]

However, the actual doctor-patient relationship imposes a more complex reflection. First, this relationship is realized, with a significant frequency, within complex organizational structures, both public and private. Also, as a result, the therapeutic activity is not carried out entirely by a single healthcare professional, but with the complicity of different actors. In this minimum and partly discounted coordinates, the need to record patient information and the problem of a regulated sharing could arise. Already in this perspective, the patient's confidentiality cannot be protected only by the professional secret, but it requires a specific health data protection regulation, to which every privacy law, by now traditionally, pays special attention.[23]

In the e-health systems the data processing plays a different and wider role. The quantitative increase of records and the computational possibilities change the landscape. The recording of data, in fact, does not only reflect the organizational purposes of the structure but directly affects the therapy, also because of the appearance of artificial intelligence as a possible 'third actor' of the doctor-patient relationship.[24] In an e-health system, the data of the individual can be

[22] About the Hippocratic oath, D Cantor (ed.), *Reinventing Hippocrates* (Routledge 2016); on its relevance in new world H. Askitopoulou, A.N. Vgontzas, 'The Relevance of the Hippocratic Oath to the Ethical and Moral Values of Contemporary Medicine. Part II: Interpretation of the Hippocratic Oath Today's Perspective', (2018) 27 Eur Spine J 1491.

[23] The statement that health data are a special category is common to the previous systems, specially to the ones based on the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, in which, according to art. 8, «Member States shall prohibit […] the processing of data concerning health or sex life», but this prohibition should «not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy»; in the GDPR, art. 9 states that «the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited», but this paragraph shall not apply in some other specific case, such as when «processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices», when there's a specific consent of the data subject, or other cases generally attributable to reasons of public interest.

[24] On the idea of Artificial Intelligence as a 'third actor' in medicine, C. Brall, P. Schröder-Bäck, E. Maeckelberghe, 'Ethical aspects of digital health from a justice point of view' (2019) 29(3) Eur J Pub Health 18.

used, together with those of others, for the acquisition of new knowledge. The model, however, has a direct impact on individual health, as in the case of personalized medicine, giving back some recommendations to the individual, following statistically oriented risk assessments. [25]

Furthermore, an artificial intelligence system can provide support in diagnostic or intervention techniques. The risks of error are significant, and the management of the possible consequences involves issues of responsibility, which are also recorded in other areas of new technologies, from robotics to artificial intelligence in general. [26] As a consequence of this statement, the new Regulation doesn't require anymore, in any case, the consent of the subject and the prior approval of Authorities, as in the previous system. [27]

In fact, according to GDPR, the processing of health data for medical purposes has an autonomous basis of lawfulness, an alternative to the consent. In other words, special categories of data can be processed, including those concerning health, or according to the consent of the data subject (as in the case of medical apps), or according to other specific reasons, as when the processing is necessary for a medical treatment (again, art. 9, letter h). [28] In the case of therapy, for example, there is no more need for the consent to the processing, because the activity requires the processing. In any case, except some 'involuntary treatment' (medical treatment undertaken without the consent of the person), the doctor-patient relationship is based on the informed consent. For this reason, the consent to data processing is somehow involved in the bigger consent to therapy, in the general framework of the relation doctor-patient.

That is why, the obligation of confidentiality of the doctor and, more generally, of the health professional and her/his collaborators gains in today's context a greater gravity than in the past. The protection of confidentiality in the ethical framework is no longer resolved only in an obligation 'not to do', in the prohibi-

---

[25] On the possibility to use big data and profiling to a risk assessment in e-health, L Lella et al., 'Predictive AI Models for the Personalized Medicine' (2019) Biostec Healthinf 199; in the psychiatric field, L. Barrigon et al., 'Precision medicine and suicide: an opportunity for digital health. Reports' (2019) 21(12) Curr Psychiatry Rep 131.

[26] On these issues, C. Allen, I Smit, W Wallach, 'Artificial Morality: Top–down, Bottom–up, and Hybrid Approaches (2005) 7(3) Ethics Inf Tech 149; or D.G. Johnson, 'Technology with No Human Responsibility?' (2015) 127 J Bus Ethics 707.

[27] On the effectiveness of consent, also in a perspective of interaction design, see L. Gatt, R. Montanari, I.A. Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Pol dir 337.

[28] The different system between medical apps and usual doctor-patient relationship is confirmed by the Italian Authority, Garante Privacy, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019*, n. 55 /2019.

tion of disclosure of patient information. That means that the protection of confidentiality takes place, also on a deontological level, in compliance with the principles and obligations set in the new Regulation. Therefore, the deontological horizon of the healthcare professional is no longer described just by reference to professional secrecy, but it is achieved primarily through active and complex conduct. Because of this, in the new Regulation, the codes of conduct are more important than in the past, thus entrusting the actors of health data processing with a guaranteed role. [29] The GDPR recognize a diffused power, which is implemented within the framework of private self-regulation and soft law. [30]

3. A human-centred technology? The *naïve* approach to the balance of fundamental rights

It is now necessary to attend the plan of possible solutions for the regulation of e-health, considering the change of the concepts of privacy and health in the new framework. This specific question is related to two general issues: the regulation of artificial intelligence and the impact of new technologies on the categories used in the bio-legal field. Both issues can be treated with a general and common theoretical approach, because there is a common background, in terms of risks for fundamental rights and use of soft law instruments.

In the first analysis, the theme of transparency is central. But behind the call for transparency, various conflicts are concealed, for the most part unsolved: protection of software ownership and the right to be known by the interested; patient confidentiality and ambition to make use of the progress determined by information sharing, etc. [31] In this context, it is only useful to recall the progressive erosion of the principle of pseudo-anonymisation in scientific research. [32]

---

[29] N. Miniscalco, 'Le regole deontologiche nella disciplina della privacy', in S. Scagliarini (ed.) *Il "nuovo" codice in materia di protezione dei dati personali* (Giappichelli 2019) 39.

[30] On soft law instruments entrusted by GDPR, L. Floridi, 'Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage' (2018) 31(2) Phil & Tech 163–167; or also B McCall, 'What does the GDPR mean for the medical community' (2018) 391 Lancet 1249.

[31] E. Vayena et al., 'Policy implications of big data in the health sector' (2018) 96 Bulletin WHO 66; T. Wykes, S. Schueller, 'Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces' (2019) 21(5) J Med Int Res e12390

[32] H.T. Tavani, F.S. Grodzinsky, 'Responding to Some Challenges Posed by the Re-identification of Anonymized Personal Data' (2019) *Computer Ethics-Philosophical Enquiry (CEPE) Proceedings* 2.

The pseudo-anonymisation is a technique contrary to the profiling mechanisms of e-health models and in any case, useless due to the significant probability of re-identification of the anonymized data. This results in a paradoxical effect: a person's private life becomes transparent, while the 'machine' that investigates it and orients meaningful choices, be they public or private, stays unknowable. [33]

This occurs both because of the individual's inability to understand the complexity of artificial intelligence software, and because of the objective 'unfathomability of the algorithm's reasons', which in the case of deep learning, are lost in overlapping data classification levels. [34]

The transparency of the software and the completeness of information aim to perform, then, an instrumental function for the responsibility and the control of the activities. Nonetheless, the framework of the Regulation is so wide and undefined that isn't that simple to understand the direct application. The main consequence could consist of the attribution of normative value to practices or standards. [35] In the case of private medical research, this is a very risky regulatory hypothesis, even for intuitive reasons.

In the same way, the appeal to the quality of technology, to the state of the art as a criterion for evaluating the protections, must be considered problematic. Art. 32 GDPR states that the appropriate measures are adopted, "taking into account the state of the art and the costs of implementation and the nature, scope, context and purpose of processing". In this case, the presumption of a too high technological standard would have prevented the access of new and small players to the digital market. Thus, the need for protection of competition and the creation of a stronger European digital market led to a more flexible solution, as opposed to the concept of standards. The expected quality is commensurate case by case. This certainly allows and greater sensitivity to competition and greater flexibility. However, the real risk is that the 'state of the art' could be a moveable standard and, therefore, too often the opposite of a standard rule.

Finally, in several documentations of ethics and law of artificial intelligence, there is great attention to the risk of discriminatory effects of the algorithms and to the potential impact on fundamental rights. [36] At this level we find the es-

[33] On the relevance of the 'knowability of the aglorithm', see G De Minico, 'Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria' (2019) 1 Dir Pubbl 89.

[34] M. Ananny, K Crawford 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' (2018) 20(3) New media & Soc 973.

[35] B. Toebes, 'Global health law: defining the field', in GL Burci, Id. (eds.), *Research Handbook on Global Health Law* (Edward Elgar Publishing 2018) 2.

[36] On this topic T.B. Gillis, J.L. Spiess, 'Big Data and Discrimination' (2019) 86(2) University Chicago Law Rev 459; in medical field WN Price, IG Cohen, 'Privacy in the age of medical big data' (2019) 25(1) Nature med 37; in this review, A. Fabrocini, 'Artificial Intelligence, Data

sence of every appeal to the construction of a human-centred technology: in this sense, the principle of equality (or equal protection clause), the protection of fundamental rights and a variable set of philosophical and juridical values are evoked. However, these appeals seem to outline a sort of coexistence of fundamental rights, almost a harmony that excludes potential conflicts, sometimes with a generic reference to the concept of dignity.[37] It is true, in the opposite, that both equality and fundamental rights involve frequent conflicts and necessary operations of balance.[38] This balancing operation is usually made by the democratic decision of a parliament, or at least, by supreme or constitutional courts. It could be too hard to expect all these sensitivities in a software programmer and some of these appeals refers to a naïve approach to the problem, if not a sort of 'do-gooder method'.

Legislative power often appears unsuitable for the regulation of technological progress, from many points of view and first because of its slowness.[39] For other reasons, it is not possible to rely only on the power of the courts, that too often enforces practices of the privates. Besides, we could underline the role of public para-jurisdictional bodies, such as independent authorities, which have several regulatory instruments.[40] Even authorities need to recover elsewhere the

---

Protection and Privacy: European Parliament Resolution of 12 February 2019 on "A comprehensive European industrial policy on artificial intelligence and robotics' (2019) EJPLT News 30.04.2019.

[37] For a view of this concept in our legal doctrine, see also A. Pirozzoli, *La dignità dell'uomo. Geometrie costituzionali* (ESI, 2012) 184.

[38] See also O. Pollicino, O. Soldatov, 'Judicial Balancing of Human Rights Online', in M. Susi (ed.), *Routledge Handbook on Digital Society, Human Rights and Law* (Routledge 2019); in medical research, H.B. Bentzen, N Høstmælingen, 'Balancing Protection and Free Movement of Personal Data: the New European Union General Data Protection Regulation' (2019) 170(5) Ann Int Med 335; for the balance in Italian doctrine, see G. Zagrebelsky, *Il diritto mite. Leggi diritti giustizia* (Einaudi 1992), and R Bin, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzional* (Giuffrè 1992); see also F. Modugno, *I nuovi diritti nella giurisprudenza costituzionale* (Giappichelli 1995) 94; or Id., 'Interpretazione per valori e interpretazione costituzionale', in G. Azzariti (ed.), *Interpretazione costituzionale* (Giappichelli 2007) 51, *contra*, in the same book, A Pace, 'Interpretazione costituzionale e interpretazione per valori', 83; shortly G. Pino, 'Conflitto e bilanciamento tra diritti fondamentali. Una mappa dei problemi' (2006) 1 Et & Pol 1; on the legal concept of 'value' in continental legal culture, see A. Longo, *I valori costituzionali come categoria dogmatica*, (Jovene 2007) 110; recently and focused on law and new technologies, see G. Resta, *Diritti fondamentali e diritto privato nel contesto digitale*, in F Caggia, Id. (eds.), *I diritti fondamentali in Europa e il diritto privato* (Roma TRE-Press 2019) 117.

[39] S. Sileoni, *Autori delle proprie regole I codici di condotta per il trattamento dei dati personali e il sistema delle fonti* (CEDAM 2011); A. Iannuzzi, *Il diritto capovolto* (Editoriale Scientifica) 2018.

[40] C. Etteldorf, 'Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules' (2018) 4 Eur Data Prot Law Rev 235.

rules to apply; but they can't rely just on legislation, hard law instruments or, again, on private standards.

Temporary conclusions

It is clear that the complexity and importance of this set of problems cannot be only managed by the self-regulation of private individuals, not because they pursue dark or illegal interests, but because the privately-owned enterprises cannot take on the framework of values, principles and rights we are dealing with. The appeal to the role of the public actors seems to be appropriate in the regulation of this sector.

There are currently no definitive solutions. Therefore, the scientific and lawyer communities are called to a particular commitment: to define a new *nomos* of the digital space. [41] They should gain a specific role in the complex geometry of soft law instruments and try to translate the temporary results of the scientific research in concrete patterns that can be used by the community of professionals and programmers. Specific patterns could mean documents, practical management models, governance models for companies or deliverables as a result of collective projects. [42] In the case of health, medicine, medical research and the protection of health data, this hypothesis requires the collaboration of scientists coming from different fields, from computer science to law, from bioethics to medicine.

[41] The concept of nomos also could refer to the approach of A von Bogdandy, S Hinghofer-Szalkay, 'European Public Law – Lessons from the Concept's Past', in Id., S. Cassese, P.M. Huber (eds.), *The Administrative State* (Oxford University Press 2017) 30; see also A. von Bogdandy, 'Il diritto amministrativo nello spazio giuridico europeo: cosa cambia e cosa rimane', in Id., P. Schiera, S. Cassese, *Lo Stato e il suo diritto* (Il Mulino 2013) 97.

[42] I. Carr et al., *Ethical design. At the Interface of Ethics for Big Data and the European Union's General Data Protection Regulation: deliverable D13. 2* (EU 2018).

INCOMPATIBILITIES OF THE INTRODUCTION OF THE NEW DATA PROTECTION RULES APPLIED TO THE SPANISH ELECTORAL SYSTEM IN THE LIGHT OF STC 76/2019

Noel Armas Castilla

Abstract

Data protection is a particularly relevant subject for the protection of fundamental rights such as the privacy of individuals. This right must be especially protected in the field of electoral processes, where Spanish legislation has undergone some changes that are analysed in this article. In this sense, the focus of this paper is on the recent judgement of the Spanish Constitutional Court, which annuls article 58.1 bis LOREG for incompatibility with the constitutional ordination and with certain aspects of European and national legislation on the matter. As a result, this paper tries to contribute to the discussion about this recent judgement as well as to determinate the implications of this constitutional incompatibility in the matter of data protection applied to electoral processes.

Keyword: Electoral system; data protection; unconstitutionality; regulation; data protection agency; constitutional court.

1. Introduction

The use and management of personal data are increasingly adapting to a new framework of European and national rules, as several previous papers have announced [1]. It is for this reason that legal doctrine and case law are beginning to

[1] García Mexía, P. (2016). La singular naturaleza jurídica del reglamento general de protección de datos de la UE, sus efectos en el acervo nacional sobre protección de datos. El Reglamen-

look closely at new developments in recently adopted data protection laws, namely Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter RGPD, which has provoked the publication of the organic law 3/2018, of 5 December, on the protection of personal data and the guarantee of digital rights (hereinafter LOPD).

Because of this, it is interesting to emphasize that European and national rules are related to personal data procedures in order to introduce the purpose of this paper. As can be seen by the date LOPD, the adoption of the law is a fairly recent development, which has led to some doubts and debates on the application of certain parts of the text.

So, by way of introduction, the Spanish legislative landscape has had to adapt in recent months to new regulations on data protection, especially in order to harmonise its legislation with the European one. This need motivated the approval of the LOPD in 2018, repealing the previous law of 1999, and modifying related laws such as Organic Law 5/1985, of 19 June, on the General Electoral System (hereinafter LOREG), whose implications are analysed with the aim of contributing to solve the lack of previous research in this field.

2. The Spanish framework

The Final Provisions LOPD imposed the modification of some laws concerning data protection [2], and, in fact, we are able to announce the collaboration with Universidad de Santiago de Compostela to elaborate another research analysing the normative changes whose publication is in process at this moment. As far as we are concerned in this paper, LOREG had to be modified to adapt to the mandate of the Third Final Provision LOPD. This modification consisted in the reissue of article 39.3 LOREG and the adoption of a new article, 58 bis LOREG which reads as follows:

"*Article fifty-eight bis. Use of technological means and personal data in electoral activities.*

to General de Protección de Datos, hacia un nuevo modelo de privacidad de datos (págs. 23 y siguientes). Madrid. Editorial Reus.

[2] Arenas Ramiro, M., Ortega Giménez, A., *Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Editorial Sepín, Madrid, 2019, pág. 552.

1. The collection of personal data relating to the political opinions of persons carried out by political parties in the framework of their electoral activities shall be in the public interest only where adequate safeguards are provided.

2. Political parties, coalitions and electoral groupings may use personal data obtained from websites and other publicly accessible sources for the conduct of political activities during the electoral period.

3. The sending of electoral propaganda by electronic means or messaging systems and the contracting of electoral propaganda in social networks or equivalent media shall not be considered a commercial activity or communication.

4. The informative activities referred to above shall identify their electoral nature in a prominent manner.

5. The addressee shall be provided with a simple and free means of exercising the right of opposition".

This new article caused some expectation in the political and legal spheres because of the doubts raised about the scope, application and its consequences, which has been reflected in the public [3] opinion [4] … but the first section of the article 58 bis LOREG was particularly controversial because of the *"collection of personal data relating to the political opinions"* and the doubts about which were these *"adequate safeguards"*.

The legal answer to these doubts appeared really quickly, as the Spanish Data Protection Authority (hereinafter AEPD) issued a report in December 2018 stating that article 58 bis should "be subject to restrictive interpretation as it is an exception to the processing of special categories of personal data based on the public interest which would be covered by article 9.2 g) RGPD" [5]. This report confirmed the need to delimit the scope and specify the content of article 58 a), but did not resolve the legal doubts as demonstrated by the fact that AEPD had to publish another report (circular 1/19) to explain some of the elements of the law that would affect the electoral procedures that have taken place in Spain in spring 2019. Circular 1/19 explains some of the elements to com-

[3] Santi Cogolludo, Los partidos políticos "espiarán" los datos personales de los ciudadanos para captar votos, El Mundo, https://www.elmundo.es/espana/2018/11/20/5bf31b2d468aeb5e1e8b4648.html accesed 8 October 2019

[4] La Ley permitirá a los partidos rastrear opiniones políticas en redes sociales para personalizar la propaganda electoral, RTVE, http://www.rtve.es/noticias/20181120/ley-permitira-partidos-rastrear-opiniones-politicas-redes-sociales-para-personalizar-propaganda-electoral/1841082.shtml accesed 8 October 2019.

[5] Informe 210070/2018 Gabinete Jurídico de la Agencia Española de Protección de Datos. Available at https://www.aepd.es/prensa/2018-12-19.html and exactly at https://www.aepd.es/media/informes/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-polticos.pdf.

plete the article 58.1 bis LOREG such as subjects (political parties, federations, coalitions and groups of voters), the data than can be collected (the freely expressed political opinions of persons in the exercise of their rights to ideological freedom and freedom of expression) the time when these data can be collected (electoral period), et cetera. But it is especially interesting to emphasize the article 7 Circular 1/19, where "adequate safeguards" can be read.

These guarantees must have the following characteristics [6]:

- The principle of responsibility is established from the design and by default.
- It is mandatory to appoint a data protection officer in accordance with Article 37.1.c) of the RGPD.
- A register of processing activities should be kept according article 30 RGPD, and should be precise and clear, in accordance with the principles of fairness and transparency.
- Data protection impact assessment should be carried out when special categories of data are processed on a large scale according to article 35.3 RGPD.
- The AEPD should be consulted before processing according to article 36.1 RGPD in case of high risk processing.
- Security measures must be taken as provided for in article 32 RGPD.
- The data processor must be selected when it offers sufficient guarantees and a contract must be concluded with the content of article 28 RGPD
- The exercise of the rights of access, rectification, erasure, limitation of processing and objection shall be facilitated, in a simple and free of charge manner.
- The data protection officer must verify that the data were obtained lawfully and in compliance with all the requirements of the RGPD when data are obtained from third parties who do not act as data processors, and specially that the third party must have a standing to obtain and process these data and he also has to inform to subjects about the purpose of the data transfer to political parties.
- The person responsible must observe the content of article 22 RGPD if the persons concerned are subject of automated decisions.

Several commentaries can be drawn from this list of guarantees, but maybe the most relevant conclusion is to emphasize the constant reference to the

[6] Circular 1/2019, de 7 de marzo, de la AEPD, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2019-3423.

RGPD, which means, firstly, that European legislation is a fundamental source of data protection in Spain, and secondly, that effectively both the LOPD and the LOREG could not complete the content of article 58.1 bis LOREG, which would explain why it was so necessary to observe the European regulation.

3. Position of the Spanish Constitutional Court (TC)

On the occasion of this dubious interpretation, the Spanish Ombudsman (hereinafter DP) asked TC about the constitutionality of the rule [7-8]. TC admitted the matter [9] for processing [10], collecting the background and formulating a list of very interesting legal considerations: TC recognized that political opinions are sensitive data, limiting the faculty to violate some aspects of this space of the privacy of the citizens by political parties.

For this purpose, TC explains the background of the case and summarizes one of the main concerns that caused the Spanish Ombudsman to bring the present appeal, such as the concurrence of numerous doubts that compromise the guarantees of protection of data as sensitive as political opinions. In this sense, according to STC 76/2019, "the Ombudsman argues that the legislator does not limit the processing of personal data that reveal political opinions by political parties in the framework of their electoral activities, and does not establish which guarantees are referred to in the contested provision, nor the criteria for determining them, nor the regulatory vehicle that must contain them, nor the authority or public power that must establish them, and does not even make any reference to the rights of data subjects or to the manner and conditions in which they may exercise them", which violates 18.4 CE, 9.3 CE, 14 CE, 16 CE, 20 CE, 23 CE.

---

[7] Ignacio Gil, El Defensor del Pueblo recurre al Tribunal Constitucional el SPAM electoral, ABC, 6 March 2019 https://www.abc.es/tecnologia/redes/abci-defensor-pueblo-recurre-tribunalconstitucional-spam-electoral-201903051509_noticia.html accesed accesed 8 october 2019.

[8] El Defensor del Pueblo recurre la ley que permite a los partidos políticos recopilar datos de usuarios que opinan en la red, El País, 5 march 2019, https://elpais.com/politica/2019/03/05/actualidad/1551794515_204840.html accesed 8 october 2019.

[9] El Tribunal Constitucional admite a trámite el recurso del defensor del pueblo contra el SPAM electoral, AB, 15 March 2019, https://www.abc.es/tecnologia/redes/abci-tribunal-constitucional-admite-recurso-defensor-pueblo-contra-spam-electoral-201903121347_noticia.html.accesed 8 October 2019.

[10] El Constitucional admite el recurso del Defensor del Pueblo contra el rastreo de opiniones políticas con fines electoralistas, Público, 12 March 2019, https://www.publico.es/sociedad/proteccion-datos-constitucional-admite-recurso-defensor-pueblo-rastreo-opiniones-politicas-fines-electoralistas.html accedes 8 October 2019.

These articles protect fundamental rights such as data protection, legal certainty, freedom of expression, ideology, equality, and even the content of Article 9.1 of the European Regulation, concerning the special category of data relating to political opinion.

Despite this previous background, Spanish State Attorney considers there is "an undoubted public interest" and adequate guarantees are given by the Law, giving as an example the case of "*Cambridge analytica*" and calling on the need to regulate the sector. In addition, the Spanish State Attorney considers that data collection limits are already set out in recital 56 of RGPD, LOPD and AEPD reports.

In this way, TC resolved this dispute. With that in mind, TC remembered its own doctrine to state his position on the matter:

Firstly, TC exposed in the legal basis 5-9 in STC 292/2000 [11], to fix its position about the **violated data protection**, as the right to consent to the collection of, access to, storage and processing of personal data and to their possible use or uses by a third party such as the State or an individual. It implies the right to know at all times who has such personal data and what use is subjecting them, as well as to be able to oppose such possession and uses.

Secondly, TC remembers STC 120/1992, in order to fix his position about **violated ideological freedom**, which "is not limited to adopting a certain intellectual position with regard to life and all that concerns it and to representing or judging reality according to personal convictions, in an internal dimension. This freedom also includes an external dimension of *agere licere*, in accordance with one's own ideas, without suffering sanction or demerit for it, nor suffering compulsion or interference from public authorities" (STC 120/1992, 27 June , eigth legal basis); so TC imposes two requirements: on the one hand, ideological freedom can only be intervened by rule with the rank of law, and on the other hand, this law must concentrate all the appropriate guarantees that provide legal certainty exposed at several judgments as STC 49/1999 (at his fourth legal basis)

In this sense, TC requires adequate technical, organizational and procedural guarantees to prevent risks of varying probability and severity and mitigate their effects, because just in this way the essential content of the fundamental right can be protected [12].

Furthermore, TC analyses European case law to complete judgment according the complements of the European legal sources. TC exposes on paragraph

[11] STC 292/2000, de 30 de noviembre. BOE núm. 4, de 4 de enero de 2001, páginas 104 a 118 (15 págs.).

[12] STC 76/2019, de 22 de mayo de 2019. Recurso de inconstitucionalidad 1405-2019. BOE núm. 151, de 25 de junio de 2019, págs. 67678 a 67700.

54 of Judgment of the Court (Grand Chamber), 8 April 2014, which reads as follow: "Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99)". [13]

TC does not appreciate the guarantees required for the protection of data on political opinion in the rules of data protection or electoral regulation, and therefore considers that there is a high degree of legal uncertainty. This demand for extra security is due to the fact that the freedoms violated are fundamental rights, and TC considers that the content of art. 58.1 bis LOREG is insufficient to determine whether the operations that political parties may carry out will be "the foreseeable result of the reasonable application of what was decided by the legislator" or not. So, definitely, the purpose or the legal good is not justified by the legislator, so this restriction of the right to the protection of personal data cannot be allowed. TC neither understands the conditions which may limit this right, what does not provide legal certainty.

Finally, TC concludes that "political opinions are sensitive personal data whose need for protection is, greater than other personal data. Adequate and specific protection against processing is, in short, a constitutional requirement, without prejudice to the fact that, as we have seen, it also represents a requirement deriving from European Union law. Therefore, the legislator is constitutionally obliged to adapt the protection afforded to such personal data, where appropriate, by imposing greater requirements so that they may be processed and providing specific guarantees in their processing, in addition to those that may be common or general".

4. Conclusion

As a conclusion, we are able to consider that the irruption of the technological innovations that allow a better and greater use of data have brought with

[13] STJUE (Gran Sala) de 8 de abril de 2014. Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros. ECLI identifier: ECLI:EU:C:2014:238. Available at: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A62012CJ0293

them a new legal framework that must be studied and implemented.

These laws have to regulate a technical reality that develops faster than the legislator's capacity to assimilate and manage these novelties. Therefore, some aspects of these standards have to find their pacific place in the constitutional ordination in accordance with the standards of internal and, of course, European rules that the Spanish constitution assumes as its own.

That is why the TC is based on national and European rules to resolve the incompatibility of article 58.1 bis due to the lack of guarantee in the protection of a sensitive right as the political opinions of individuals, deciding to expel it from the Spanish legal system.

LOCATION DATA PRIVACY ON MAAS UNDER GDPR

Erion Murati e Manjola Hënkoja

Abstract

Mobility as a Service (MaaS) is a new transport paradigm that integrates existing and new mobility services into one single digital platform, providing customised door-to-door transport and offering personalised trip planning and payment options. The development of MaaS relies heavily on access to user's data, open APIs of transport providers and interoperability of the systems. Since data are the key factor of MaaS, establishing clear and fair rules for the control of information is crucial. MaaS is a location-based service (LBS) navigation which uses real-time geo-data from a mobile device to provide user's location and other information. Under Article 4 of the GDPR, location data is expressly mentioned as a factor by reference to which a person may be directly or indirectly identified, thus is recognised as an 'identifier' of personal data. The aim of this chapter is to overview and analyse the privacy vulnerabilities of location data which may become sensitive data on MaaS in combination with other information. Further, this paper will analyse the guarantees provided by GDPR, either strictly legal (i.e. consent of the data subject) or technological (i.e. DPIA) and their reliability to protect user's identity.

Key-words: Navigation apps, Location Based Services, Data Location, MaaS, DPIA.

1. Introduction

An old saying says that the key to making it through life is to know where you are, where you've been, and where you're going. In today's digital world, there is an app for that. Advances in ICTs have enabled significant developments in geo-localization systems, which are increasingly embedded in smartphones and have paved the way for the development of new transport op-

tions [1] relying on the sharing of a specific asset (which can be a vehicle) or of a dedicated service (i.e. a ride), that is to say new consumption patterns. Recent research confirms an emerging picture of a possible correlation between the growth momentum of new mobility service providers and their relative dependence on mobile ICT, whereby those companies with the greatest dependence on smartphones and mobile apps are those attracting the most funds and developing the fastest. [2] Shared mobility clearly stress access over ownership and highlight the role of ICT in its development. More people are starting their trips with smartphones [3] to plan routes, seek departure information for the next bus or railcar, find a taxi via an e-Hail app, or source a private driver through services, such as Uber. Factors driving transportation app growth include: time savings (e.g., high occupancy vehicle lanes available to users of dynamic ridesharing); financial savings (e.g., dynamic pricing providing discounts for peak and off-peak travel and for choosing low-volume routes); incentives (e.g., offering points, discounts, or lotteries). For public agencies, transportation apps can aid network management functions, such as disseminating roadway and public transportation information on incidents, delays, congestion, and service disruptions. [4] For mobility users, the purpose of these apps is to facilitate door-to-door mobility by giving people greater control over their trips, through "real-time" access information and coordination, previously unavailable [5] (such as estimated departure and arrival times, comparison of routes and modal options.). Moreover, scientific research studies suggest that ICT technology is influencing traveller's behaviour when it comes to transportation choices. Reliable and tailored information, offered by ICT, allow users to make active decisions, thereby exercising a form of control on their personal outcomes. [6] This emerging mobility

[1] M. Finger, M. Audouin, *The Governance of Smart Transportation Systems Towards New Organizational Structures for the Development of Shared, Automated, Electric and Integrated Mobility* (Springer 2019) 2.

[2] V. Boutile, 'New Mobility Services', in A Aguilera, V Boutile, *Urban Mobility and the Smartphone*, (Elsevier 2018), 40-45.

[3] H. Pfriemer, 'The Digital Economy and the Promise of a New Mobility' in B Flügge (ed.), *Smart Mobility – Connecting Everyone* (Springer 2017) 73.

[4] S. Shaheen, S. Cohen, A. Martin, 'Smartphone app evolution and early understanding from a multimodal app user survey', in G Meyer and S Shaheen, *Disrupting Mobility* (Springer 2017) 150.

[5] A. Aguilera, 'Smartphone and Individual Travel Behaviour', in A. Aguilera, V. Boutile, *Urban Mobility and the Smartphone* (Elsevier 2018) 7-8.

[6] A.L. Davidson, (2017) 'Getting Around with Maps and Apps: How ICT Sways Mode Choice' in G Meyer, S Shaheen, *Disrupting Mobility* (Springer 2017) 178; See also, D Ettema, *Apps, activities and travel: an conceptual exploration based on activity theory* (Springer Transportation 2018) V 45, 273-290.

ecosystem can deliver many benefits for traditional transport service providers as well, including integrated payment scheme, developing better first-mile/last-mile and enhancing the richness of transportation data. [7]

Mobility as a Service (MaaS) concept has risen from the recent mobility tendency, promising an integrated flexible mobility platform. [8] The complexity of using a variety of transport modes, different payment methods and lack of integrated information discourages many people from using them. The key is to integrate the various transport modes in a way that creates seamless door to door journey experiences for users through a MaaS platform. Basically, integrated mobility aims to enable multimodal travel [9] – defined as the use of more than one travel mode for passenger or goods movement – and produce a shift from private motorized travel to more sustainable modes of travel such as public transport or shared mobility modes. According to Finger [10] (2019) integrated mobility has basically been facilitated recently by two main ICT-supported developments: the development of integrated multimodal information systems, and integrated payment solutions. While the former has enabled users to access and compare specific travel information in real time from different transport providers, and therefore pick the solution best fitting their mobility needs [11] the latter has enabled users to access various transportation solutions with a single ticketing means, which could be a card (smart card) or a dedicated app. Put together, and also supported by the birth of new shared mobility solutions, those two ICT-supported developments have enabled the unfolding of the Mobility-as-a-Service (MaaS) concept. Shared mobility, automated mobility, electric mobility and integrated transport are the four pillars which will contribute to shape the concept of smart mobility: zero emissions, zero accidents and zero ownership. [12] According to the House of Commons report [13] (2018) on MaaS in-

---

[7] M. Dinning, T. Weisenberger, 'Multimodal Transportation Payments Convergence-Key to Mobility' in G. Meyer and S. Shaheen, *Disrupting Mobility* (Springer 2017) 120-122.

[8] S.H. Fariya, M. Henk, 'The Governance of Demand-Responsive Transit Systems-A Multi-level perspective' in M. Finger & M. Audoin, *The Governance of Smart Transportation Systems* (Springer 2019) 1.

[9] S. Shaheen, and others, *Mobile Apps and Transportation: A Review of Smartphone Apps and A Study of User Response to Multimodal Traveler Information*, (California 2016) 13.

[10] M. Finger, M. Audouin, *The Governance of Smart Transportation Systems Towards New Organizational Structures for the Development of Shared, Automated, Electric and Integrated Mobility* (Springer 2019) 3.

[11] S. Kenyon, G Lyons, *The value of integrated multimodal traveller information and its potential contribution to modal change* (Transp. Res. 2003) 1-21.

[12] L. Neckermann, The mobility revolution zero emissions, zero accidents, zero ownership in https://www.troubador.co.uk/bookshop/computing-science-education/the-mobility-revolution/Accessed August 2019.

quiry the MaaS ecosystem is made up of: 1) customers; 2) MaaS platform providers: who design and offer the MaaS platform (app or website) and create packages based on customer demands; 3) data providers: who share and use data, which is crucial to MaaS, 4) and a range of transport operators; The combination of these new technologies allows a mobility which is in no way inferior to the freedom promised by the private car. To meet a customer's request, a MaaS operator facilitates a diverse menu of transport options, be they public transport, ride –, car – or bike-sharing, taxi, car rental or lease, or a combination thereof, accessible *on demand*. Since MaaS concept is holistic and still emerging, it can be defined and approached from many different points of view, however the definition used in this chapter is the same definition adopted in MaaSiFiE project, namely: "Multimodal and sustainable mobility services addressing customers' transport needs by integrating planning and payment on a one-stop-shop principle" [14] Since 2014 when MaaS concept was officially introduced to the public at the 2014 ITS European congress in Helsinki [15] MaaS has received much attention within and around the transportation industry. Proponents argue that MaaS will become the new transport paradigm since it addresses many of society's grand challenges in transport, promising improvements in terms of environmental sustainability, reduced congestion and better accessibility. [16] It has also been argued that the diffusion of MaaS may completely change both how we travel and how personal transportation is organized and that MaaS could be an emerging trillion-dollar industry at the expense of the incumbent private car sector. [17] However, alongside the benefits comes also the drawbacks. The main objective of this chapter is to analyse the privacy vulnerabilities of location data

[13] Mobility as a Service inquiry in https://www.parliament.uk/business/committees/committees-a-z/commons-select/transport-committee/inquiries/parliament-2017/mobility-as-a-service-17-19/Accessible December 2018.

[14] D König and others, *Deliverable 3: Business and operator models for MaaS* (MAASiFiE 2016) 1-10.

[15] M Audouin, *Towards Mobility-as-a-Service: a cross-case analysis of public authorities' roles in the development of ICT-supported integrated mobility schemes* (2019) in https://infoscience.epfl.ch/record/264957 Accessed August 2019 163.

[16] Polis, *Mobility as a service: Implications for urban and regional transport. Brussels* in Polis network 2017 Retrieved from https://www.polisnetwork.eu/uploads/Modules/PublicDocuments/polis-maas-discussion-paper-2017---final_.pdf Accessed September 2019; See also, MaaS Alliance (2017 September 4) *White Paper: Guidelines & Recommendations to create the foundations for a thriving MaaS Ecosystem* in *MaaS Alliance* 2017, Retrieved from https://maas-alliance.eu/wp-content/uploads/sites/7/2017/09/MaaS-WhitePaper_final_040917-2.pdf Accessed August 2019.

[17] G Smith and others, 'Governing Mobility-as-a-Service: Insights from Sweden and Finland' in M Finger M Audouin (eds) *The Governance of Smart Transportation Systems* (Springer 2019) 170.

and to shed lights on the impact that GDPR is having on MaaS provider which may use location data to monitor user's travel behaviour or to identify and process sensitive data patterns. In the next section the key role of data on MaaS is discussed. In section 3 the way location data is collected and used, under section 4 potential privacy risks arising to location data via LSB. Furthermore, an analyse of GDPR has been conducted in regard to the protection of personal location and/or sensitive data, with its legal remedies and technical guarantees.

2. The key role of data on MaaS

Data means (electronically) stored information, signs or indications. For MaaS to be successful a wide range of transport data is required. [18] The MaaS app basically enables customers to access information about what mobility solutions are available for the trip they are planning to make, thanks to an embedded routing system, as well as directly book the solution of their choice, and pay for it, all in the same app. From a technological perspective, MaaS providers position themselves on two different fronts. On one hand, MaaS providers basically integrate data, such as routes, real time user'/vehicle's position, speed, transfer time and as well as the application programming interfaces (APIs) of the different transport operators, both previously made open by them. APIs represent a set of processes that govern the interactions between different web-based services [19] and put together constitute what is referred to as the back-end, also sometimes called the data platform or data layer, that MaaS providers operate. Therefore, sharing of APIs allows MaaS providers to offer customers a single digital interface for planning, booking, paying for and using transport. [20] On the other hand, MaaS providers also take care of building the app and the website that comes on top of the back-end, which is the major customer interface, referred to as front-end.

The most important policy designed at the national level to enable the development of MaaS, via deregulation, is the new Finnish Transport Act, entered into force in 2018. [21] The Code focuses on enhancing the use of open data and oblige mobility operators to provide their operational data as well as their single tickets for third-party resale and use. The main idea of the Code is to take ad-

[18] M. Kamargianni, M. Matyas, *The potential of mobility as a service bundles as a mobility management tool* (Springer 2018) 1-16.

[19] D. König and others, *Deliverable 5: Technology for MaaS* (MAASiFiE 2016) 21.

[20] M. Kamargianni, *The potential of mobility as a service bundles as a mobility management tool* (n. 18) 2.

[21] LVM 2017a Finnish Transport Code. Act on Transport Services https://www.lvm.fi/lvm-site62-mahti-portlet/download?did=246709 Accessed August 2019.

vantage of digitalization and enable both the development of better and more agile transport services, and the integration of them into MaaS offerings, with the concrete goals of achieving a 10% savings in publicly subsidized passenger transport from 2017.[22] The finish transport code (2017), can be understood as a real push towards MaaS, for three main reasons. Firstly, it enables the size of the for-hire vehicles fleet to grow as any type of vehicle is allowed to be used as a taxi by removing the existing quota that has been limiting their total number of licenses in Finland (Chapter 1, Section 1). For-hire services are an important part of MaaS as they might bring a solution to the last-mile problem. Secondly, the text is seen as MaaS enabler as it forces all transport services providers to open essential data such as routes, timetables, stops, and fares in a computer-readable format (Chapter 2, section 1). Thirdly, it lays down provisions for the interoperability of ticketing systems, by requiring all public transport providers to open their single tickets APIs (Section 2). In 2018 the second part of the Code was approved (amendment n. 301/2018) and in *Section 2 a* was introduced the concept of acting in someone else's behalf, forcing transport providers to open up also seasonal tickets APIs. In a nutshell, MaaS concept lies on the idea of open data in transport industry. According to the European data portal definition[23], open data can be defined as "data that be freely used, modified, and shared by anyone for any purpose subject, at most, to measures that preserve provenance and openness". In other words, open data is data that can be accessed, shared, used and reused without any barrier for any type of (re)user. However, in a digital economy, the ownership and access to data determines the market dominance. Therefore, referring to MaaS Alliance[24] view it should be understood that data sharing does not necessarily equal to free data, but data sharing and exchange models should be designed between partners to be fair and to fit for purpose. The Code has predicted these concerns and according to Section 4, access to information and information systems offered through the open interfaces shall be offered on fair, reasonable and non-discriminatory terms. Alongside the need for data sharing and openness comes the need for data security, especially when it comes to user data. The International Transport Forum[25] (2016) outlines a number of factors which contribute to transport data

[22] G Smith and others, *Mobility as a service: Comparing developments in Sweden and Finland* (RTMB 2018) 40.

[23] European Data Portal, 2018, Open data in a nutshell https://www.europeandataportal.eu/en/providing-data/goldbook/open-data-nutshell Accessed August 2019.

[24] MaaS Alliance (2018, November) Data Makes MaaS happen, *in MaaS Alliance* https://maas-alliance.eu/wp-content/uploads/sites/7/2018/11/Data-MaaS-FINAL-after-plenary-1.pdf Accessed August 2019 Accessed August 2019.

[25] International Transport Forum, *Data Driven Transport Policy* Available at: https://www.itf

security: 1) Data minimization, collecting the minimum amount of data required and dispose it when it is no longer relevant; 2) De-identification/Anonymization, removing personal details associated with data, achieved through aggregation; 3) Encryption, encoding information so that only authorised parties can access it; 4) Transparency in "terms of use", making it clearer to people what data they are consenting to being shared.

3. Collecting and using personal location-based data

Location history is one of the prime bits of data any business can get on you, whether they want to personalize your weather reports, serve up an ad for a local restaurant or direction to parks. These services are known as location-based services (LBS) which are based on the user's current position to provide location-aware information. [26] As a result, apps and mobile Operator Systems (OS) are very keen to get hold of it. It's a compromise though, and if you don't want to give it away, you'll have to do without some location-based services (like directions to the parks, restaurants, museums and cities). The choice to be made is between convenience or privacy? You can't have both, but it is important to understand who can access this information, and what steps can be taken to ensure that only authorized parties can access it. The rise of LBSs is evident as 90 % of smartphone users polled said they used their device to find LBSs, such directions or local recommendations. [27] A recent survey by The Manifest [28] confirms that LBS navigation has become a staple for more than three-quarters of mobile users, with Google Maps being the overwhelming choice for mobile users. On MaaS ecosystem referring to scientific papers [29] real time user' and vehicle's position, allows MaaS provider to determine how far away vehicles are from customers

oecd.org/sites/default/files/docs/data-driven-transport-policy.pdf Accessed 24 August 2019. Accessed August 2019 23-26.

[26] C Bettini, S Mascetti, X Wang, 'Privacy Threats in Location-Based Services' in S. Shekhar, H. Xiong, (eds) *Encyclopedia of GIS* (Springer 2008).

[27] Marketer report (2016) Most smartphone owners use LBSs, https://www.emarketer.com/Article/Most-Smartphone-Owners-Use-Location-Based-Services/1013863 Accessed August 2019.

[28] P Riley, The popularity of Google Maps: trends in navigation Apps in 2018 (2018, July 10) https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018Accessed August 2019.

[29] Transport Systems Catapult (2016). Mobility as a Service: Exploring the opportunity for Mobility as a Service in the UK [Online] Available at: https://ts.catapult.org.uk/wpcontent/uploads/2016/07/Mobility-as-a-Service_Exploring-the-Opportunity-for-MaaS-in-the-UK- Web.pdf Accessed August 2019; See also, M. Kamargianni, M. Matyas, *The potential of mobility as a service bundles as a mobility management tool* (Springer 2018) 1-16.

and thus estimate what time they will arrive (when combined with speed data). Moreover, thanks to location data MaaS provider could capture users' historical travel behaviour to better predict future travel patterns, modelling travel behaviour to forecast how users travel in time and space, understanding also the factors that influence on travel-related choices. For instance, the MaaS provider could incentive its user to use sustainable means of transportation – i.e. bike sharing –, giving some transport credit points for each km ridden. In performing that task, MaaS provider needs to know how many km a user is riding for a certain time. GPS, Bluetooth (used the latter, for example, by Mobike app for the ride of its free flow bikes) and other dynamic data will assist MaaS provider in order to fulfil this goal. This practice takes place in Bologna, in Italy, which rewards bike runners with free beers in exchange of the credit points accumulated during the ride. [30] Finally, geodata suggest users' most convenient route to be taken or to reroute her/him in case of a transport disruption to the final destination.

Generally, the term 'location data' comprises any information implicitly or explicitly referring to geographic or geospatial position. More specifically, according to Location Forum [31] location data is any data with an implicit or explicit geographic or geospatial reference, including any data derived from GPS, GIS, cell-tower or other radio signal based triangulation, assisted GPS positioning devices, systems and processes, geo-tagged images, video, audio and text documents, satellite and aerial imagery, computerized, digitized and paper maps, IP address location, public documents, public or private databases, video, audio, text and image files, location-based applications. However, personal location data is any information about a natural person's current or past geographical location or movements. [32] Technically, the monitoring can be done secretively, without informing the owner. Monitoring can also be done semi-secretively, when people "forget" or are not properly informed that location services are switched "on", or when the accessibility settings of location data are changed from "private' to 'public". For instance, according to a recent investigation of the Guardian [33], Facebook targets users with LBSs adverts even if they block the

[30] M. Buck A Bologna birra gratis per chi si muove in bicicletta (2018 December 7) https://www.welovecycling.com/it/ciclismo-urbano/2018/12/07/a-bologna-birra-gratis-per-chi-si-muove-in-bicicletta/ Accessed August 2019.

[31] Location Forum, *Location Data Privacy Guidelines, Assessments and Recommendations* (Version 2, 1 May 2013) 7.

[32] E. Morriessey, (2016) *Data protection issues Guidance on Location Data*, in https://www.fieldfisher.ie/data-protection-office-issues-guidance-location-data/ Accessed September 2019.

[33] The Guardian, (2019) Facebook users cannot avoid location-based ads, investigation finds, https://www.theguardian.com/technology/2018/dec/19/facebook-users-avoid-location-based-adssettings-investigation-reveals Accessed September 2019.

company from accessing GPS on their phones, turn off location history in the app, hide their work location on their profile and never use the company's "check in" feature. There is no combination of settings that users can enable to prevent their location data from being used by advertisers to target them. According to Chrétien [34], within the smartphone world geolocating applications fall into two categories depending on their purpose: either "statistical" in the sense of data collected by public authorities and designed for public policy or "business." Within the "business" category, there are four kinds of purposes: 1) mobility assistants, from map location to path identification (Google Maps, Apple Plans) and en-route guidance; 2) location-based services (LBS), advising the user on the best or closest service (e.g., restaurants, shopping or touristic activities); 3) self-monitoring of activities, such as running; 4) marketing analysis of user's activities and spatial practices, so as to detect his or her consumption styles, tastes, and desires. Differently, other scholars [35] put together all geolocating applications within the concept of LBSs. However, if referred to Chrétien's classification – technically more precise-, MaaS providers could also add in their platform LBSs and marketing analysis of user's activities and spatial practices. Location information may represent some of the most sensitive data collected and stored by transportation apps and shared with third parties to offer users additional products and services. Privacy and security concerns are complicated by this type of data sharing because this is often facilitated through third-party APIs, which may contain security vulnerabilities in addition to the cloud, software, and hardware security protocols.

4. Privacy and data protection risks

The privacy risks associated with personal data being collected by data controllers are not a new phenomenon. However, the data privacy implications associated with apps are heightened beyond traditional data collection means because of apps' ability to collect data instantaneously, continuously, and often without knowledge of the user, at an extremely granular level, whether it be the

[34] J. Chrétien and others 'Using Mobile Phone Data to Observe and Understand Mobility Behaviuor, Territories, and Transport Usage' in *Urban Mobility and the Smartphone* (Elsevier 2019) 82.

[35] See S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage: An EU Law Perspective* (Helsinki (2018); C Bettini, Privacy Threats in Location-Based Services (n. 25); Article 29 WP, Opinion 13/2011 n. 185 on Geolocation services on smart mobile devices https://iapp.org/media/pdf/resource_center/wp185_Geolocation-smart-devices_052011.pdf Accessed August 2019.

exact coordinates or the specific heart rate of an individual at any given moment. This micro-level collection of data by sensors creates more pressing data privacy implications for individuals.[36] On MaaS ecosystem the digital interface between users and MaaS provider is their smartphone and in an ideal workflow, after possibly having set their preferences, they send a request and receive in response one or more "mobility solutions", they pay the ticket for the one selected. Besides leaving aside that, matching the GPS coordinates other of the smartphone with its location, the system can track users in their route, allowing it to follow his/her movements in real-time and to detect a pattern. Since the preliminary analysis on Intelligent Transport System, the real possibility that the user could be not only profiled but also "singled out" has raised many concerns, which become more sensitive in MaaS due the increasing number of interconnected databases.[37] It is important to underline that by collecting location data, MaaS provider or app developers are able to deduce many types of personal information apart from merely location, such as religious believes or political affiliation. To give an example, if a person visits a church regularly or goes to a gay bar in the weekends, conclusions can be drawn about that person's religion or sexual preferences. Because many privacy-protected attributes are uniquely associated with places or events, collecting data that show a person frequently visits a place or attends a particular event represents a powerful means to draw a comprehensive picture of an individual.[38] In such cases, location data becomes special categories of personal data or "sensitive data", such information on the frequency and place of obtaining medical care, religious activities, political orientation or sex life, that require a higher level of protection under Art. 9 GDPR and in the case of sensitive data it prohibits its dissemination by default. Only under specific conditions might such data be processed. These profiles can be used to take decisions that significantly affect the owner. Moreover, other data can be inferred through the publication of location data, for example real-time emotional and physiological status[39], and co-location (i.e. the presence of other people in the same location). In a nutshell, two fundamental rights are in risk from collecting and processing location data: first the right to privacy and sec-

[36] A. Fong, *The role of app intermediaries in protecting data privacy*, in International Journal of Law and Information Technology (2017) 85-114.

[37] F. Costantini, MaaS and GDPR: an overview (2017), in https://arxiv.org/abs/1711.02950 Accessed August 2019

[38] S Bu-Pasha and others 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' in *European Data Protection Law Review*, *2*(3/2016) 312-323

[39] D. Riboni, L. Pareschi, C. Bettini, 'Privacy in location-based applications' in *Privacy in Georeferenced Context-Aware Services: A Survey*, (Springer-Verlag 2009) 151-172.

ondly the right to data protection. Generally, the right to privacy – referred to in European law as the right to respect for private life – emerged in international human rights law in the Universal Declaration of Human Rights (UDHR), adopted in 1948, as one of the fundamental protected human rights. Soon after adoption of the UDHR, Europe too affirmed this right in article 8 of the European Convention on Human Rights (ECHR). The right of data protection emerged as a need to control collection of personal data enhanced by digitalisation. The right to respect for private life and the right to the protection of personal data are closely related. Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion.[40] The two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. According to Advocate General Sharpston[41], the protection of personal data is viewed as a modern and active right putting in place a system of checks and balances to protect individuals whenever their personal data are processed. In regard to location data privacy, according to Alastair R. Beresford and Frank Stajan[42] definition it's "the ability to prevent other parties from learning one's current or past location". Location data privacy implies the right to not be subjected to unauthorised collection, aggregation, distribution or selling of an individual or organization's location or location profile derived from location data.[43] The concept of location data privacy does not refer to hiding information – rather it safeguards one's present or past location information from use for commercial or other purposes without one's knowledge. In connection with location data, when a person loses the ability to control his or her location information, or the ability is limited somehow by another authority, that person's privacy came under threat.[44] Considering privacy principle, it is neces-

[40] Handbook on European data protection law, 2018 edition, https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law Accessed August 2019.

[41] Advocate General Sharpston, see CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

[42] R Alastair, Beresford, F Stajano, 'Location privacy in pervasive computing' in *IEEE Pervasive Computing*, 2(1): 46–55, 2003 Available online here https://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf.

[43] Location Forum, *Location Data Privacy Guidelines* (n. 30) 7.

[44] S. Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 9.*

sary to take into account participants' perception and behaviour surrounding their privacy. The "privacy paradox," which designates the fact that people declare concern for their personal information but willingly diffuse it online also applies to geolocation technologies [45] which explains the broadness of data currently available. However, this is not to say that individuals "give away" their information or location randomly: they are more likely to accept to relinquish some privacy if the website or application is entertaining, provides monetary or social benefits. [46]

5. Personal location data under GDPR

The EU's General Data Protection Regulation (GDPR) aims to change the way that consumer data is gathered and used. The GDPR applies to any processing of personal data which means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means (Art. 4 n. 2 GDPR.) However, data has to be personal in order to fall within said scope of application of the Regulation. Data is deemed personal if the information relates to an identified or identifiable individual, (Art. 4 n. 1 GDPR.) Article 4 of the GDPR recognize location data expressly as a factor by reference to which a person may be directly or indirectly identified, thus is recognised as personal data if they identify a natural person. In order to understand the role of location data under GDPR, it is important to distinguish between cases where location data constitute either personal data or sensitive data from those cases where the data are effectively anonymised, thus not considered personal data and GDPR does not apply. [47] As a personal data, the following provisions of GDPR are applicable to location data privacy. Article 5 of the GDPR states the principles to be followed in in processing personal data. The GDPR introduces the general principle of accountability in Art. 5 Sec. 2 GDPR, which imposes the responsibility for the compliance of processing with the GDPR and

[45] A.M. Zafeiropoulou, (2014) *A Paradox of Privacy: Unravelling the Reasoning Behind Online Location Sharing* (Ph.D)University of Southampton https://eprints.soton.ac.uk/376477/1/_userfiles.soton.ac.uk_Users_slb1_mydesktop_soton.ac.uk_ude_personalfiles_users_jo1d13_mydesktop_Zafeiropoulou.pdf Accessed August 2019.

[46] S Kokolakis, 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon' in *Computers & Security* 64 (2017) 122-134 https:// doi.org/10.1016/j.cose.2015.07.002 Accessed September 2019.

[47] P Voigt, & A Bussche, *The EU General Data Protection Regulation (GDPR) Handbook*, (Springer 2018) 13; Same position also, S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 64.*

the burden of proof for said compliance into the controller (Voigt & Bussche, 2018). Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (Art. 5 Sec. 1. a). Entities should first decide on the purpose of collecting data and then, by notifying the data subject about the purpose, collect data only to fulfil that purpose. Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Art. 5 Sec. 1. b). Thus, it restricts the secondary use of data. For instance, LBS app, like MaaS and Google Maps collect location data offering particular geographical location services. The GDPR makes it clear that location data collected for a particular purpose should be used for its declared purpose only. [48] Therefore, data processor or controller on MaaS cannot use that data for advertisement or any secondary purpose without an additional consent from data subject. In addition, Art. 5. (c) of GDPR establish the data minimisation principle, aiming for a reduction of data collection to the lowest possible level for realising the processing purposes by companies. According to the "storage limitation" principle in Art. 5 (f) personal data can be stored "no longer than is necessary for the purpose for which the personal data are processed". Moreover, Art. 6 of GDPR has strengthened the conditions of data processing such that processing is permitted only when it's necessary on lawful grounds.

Further concrete data protection instruments are being prescribed in Art. 25 GDPR: companies should use the concepts of Privacy by Design and Privacy by Default. It means that entities and organizations should adopt appropriate technical and organizational measures from the beginning of the service. Privacy by Design (Art. 25 Sec. 1 GDPR) is based on the realisation that the conditions for data processing are fundamentally being set by the soft and hardware used for the task. When creating new technology, developers and producers shall be obliged to keep data minimisation in mind. However, data protection by design is about complying with GDPR as a whole and the most effective way of discharging the controller's burden of that compliance is to avoid processing personal data in the first place, like pseudonymisation. [49] On the other hand, the concept of Privacy by Default (Art. 25 Sec. 2 GDPR) shall protect consumers against the widespread trend among companies to obtain as much personal data as possible. [50] By default, only personal data that are necessary for the specific

[48] Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 38.*

[49] For more information see D Kelleher, M Karen, EU Data Protection Law (Bloomsbury Professional 2018)267.

[50] P. Voigt, A Bussche, *The EU General Data Protection Regulation* (n. 46) 63

purpose of the data processing shall be obtained. Where users wish to change settings of a service, e.g. to allow further use of or share their personal data with more parties, they should have to opt in and amend the settings by themselves.

Data subject has under GDPR a set of rights over his or her data. According to the Handbook on European data protection law [51] first of all, controllers of processing operations are obliged to inform the data subject at the time when personal data are collected about their intended processing. As data processing can negatively impair the rights and freedoms of data subjects, especially where it is unlawful or where it involves incorrect or incomplete data, the GDPR provides for different rights of data subjects that permit them to limit or influence processing activities carried out by the controller. These rights are the right to rectification, the right to consent, the right to erasure and the right to restriction of processing. Article 20 GDPR introduces a new data subject right, the right to data portability which is the right for customers to transfer their data from one data system to another and is extremely important for MaaS. According to Transport Systems Catapult [52] this means that customers can switch MaaS providers encouraging a competitive market which supports innovation, quality assurance and the delivery of value for money. The GDPR also outlines the responsibilities of data holders such as the responsibilities to encrypt and anonymise data, report data breaches, and record processing activities.

5.1. Sensitive location data

Generally, location data are not sensitive but can disclose sensitive information in association with other information, tending to become sensitive data under EU data protection law [53] (Bu Pasha, 2018) with special legal effects (Art. 9 GDPR). Those special categories of personal data merit specific protection as they allow conclusions about an individual that are linked to his fundamental rights and freedoms, and their processing might entail high risks for the latter. Deducing user's sensitive patterns (data) on MaaS is easier whenever data location is combined with user's ID name, email address, telephone number, physical address, account number, credit cart, which are identifying personal data.

[51] *Handbook on European data protection law*, (n. 39) 111.

[52] Transport Systems Catapult (2016). Mobility as a Service: Exploring the opportunity for Mobility as a Service in the UK [Online] Available at: https://ts.catapult.org.uk/wpcontent/uploads/2016/07/Mobility-as-a-Service_Exploring-the-Opportunity-for-MaaS-in-the-UK- Web.pdf Accessed August 2019

[53] Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 47.*

Moreover, the risk increase considering that MaaS app access phone's identifiers, such as International mobile equipment identity and Identity management system, which, as shown by Enck [54], are among the most commonly used sensitive data that app collects. One of the reasons why MaaS provider needs to have such personal data is because some tickets or monthly subscriptions are personalized and valid only for special type of users. (i.e. student card). Location data on MaaS are highly valuable to a number of interested parties with diverse intentions and purposes, ranging from advertisers to car manufacturers, transport operators and public transport management authorities. For instance, in order to avoid traffic jams transport authorities can develop models to forecast how user travel in time and space, and to understand the factors that influence on travel-related choices. However, unrestricted and indiscriminate access to data shared may allow for the unfair accumulation of individual movement profiles, a "datification" of pattern behaviours on which personalized goods and services can be shaped, advertised and sold [55] (WP29 n. 252, 2017). From a GDPR point of view, it's not clear for example how data concerning trips to hospitals (or to other sensitive places) could be lawfully treated in MaaS, since they would qualify as "data concerning health" by Article 4 n. 1 (15) of GDPR and they would fall into the prohibition of Article 9 n.1 of GDPR. Considering that MaaS could identify user's sensitive patterns, whenever monitoring a user's travel destination through location data which may reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data or biometric data, data concerning health or data concerning a natural person's sexual orientation processing shall be prohibited by default under Art. 9 of GDPR. Nevertheless, the provision introduces several exceptions from the prohibition of processing special categories of personal data (i.e. consent of data subject). Data subject can explicitly consent to the processing of special categories of personal data for one or more specified purposes. Such affirmative act not only has to fulfil the general conditions for valid consent under Arts. 7, 8 GDPR but also has to explicitly refer to the special categories of personal data concerned by the intended processing. [56]

[54] W. Enck, D. Octeau, P. McDaniel, S. Chaudhuri, 'A Study of Android Application Security' in *Proceedings of the 20th USENIX Security Symposium (USENIX Security 2011)*, 1-16.

[55] Article 29 WP, n. 252, (10/2017) Guidelines on Processing personal data in the context of cooperative Intelligent Transport System https://ec.europa.eu › newsroom › just › document Accessed August 2019, 8.

[56] P. Voigt, A. Bussche, *The EU General Data Protection Regulation* (n. 46) 112.

5.2. Legal justifications for location data processing

Article 6 of GDPR sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose. [57] Different roles are involved in the processing of personal data. A controller defines the purposes and methods of processing personal data, independently or together with others (Art. 24 GDPR). A processor processes personal data on behalf of the controller. In this case, processing is commissioned or subject to subcontracting or a partnership (Art. 28 GDPR). There can also be parallel controllers, in which case each controller has an independent right to process personal data (Art. 26. GDPR). The processor does not have any independent right to use the data. The controller must notify data subjects of any processing of personal data. This information includes the controller's contact details, information about the purpose and principles of data processing, and information about the rights of the data subjects. (Art. 13 GDPR). The provider of a MaaS application that is capable of processing geolocation data is the controller for the processing of personal data resulting from the installation and use of the application, independently from the developer of the operating system and/or the controllers of geolocation. Basically, any treatment of data will be considered as processing. Examples include collecting, recording, organising, structuring, storing and erasing of data.

A common regulatory challenge around transport platforms is to define their legal status which may also reflect the roles involved in the processing of personal data. In particular, the debate has focused on whether they provide an intermediation service using digital technology, or they really provide a full transportation service, for which a license is often required, and full liability before passengers has to be ensure. This has been the case of Uber considered by European Court of Justice as transport provider instead of mere intermediary service. [58] In MaaS ecosystem, the MaaS operator, being the transport provider, acts as the controller regarding personal data collected from passengers. On the other hand, the MaaS operator being the intermediary, and transport service providers can act as controllers and/or processors, depending on which data is being processed and what has been agreed upon regarding the tasks and roles of

[57] Article 29 WP n. 259, 12/2017 on Guidelines on Consent under Regulation 2016/679 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 Accessed September 2019

[58] See J. Montero, 'Regulating Transport Platforms: The Case of Carpooling in Europe' in M. Finger, M. Audoin, *The Governance of Smart Transportation Systems* (Springer 2019) 11-25

each party. Deviating from any roles defined in legislation is not possible. Generally, for MaaS provider with regard to the legal basis for data processing, three different possibilities seem to be more suitable to be applied [59]: Art. 6 (1) (a) of GDPR (consent by the data subject), Art. 6 (1) (b) of GDPR (performance of a contract) or Art. 6 (1) (f) of GDPR (legitimate interest). In specific, Bu Pasha (2018) in her work had considered consent as the easiest way to process location data through, on one hand, providing notice of the users about the way, extent and possibility of collection and processing of their location data, on the other hand, seeking their consent. Therefore, whenever processing of (patterns of) location data is based on consent, the MaaS data controller shall be able to demonstrate that the data subject has consented to the processing, (Art. 7. Sec. 1 GDPR). Thus, it bears the burden of proof, for example, if a data subject claims to have given no or no valid consent, which corresponds to the controller's accountability under Art. 5 Sec. 2 GDPR for the lawfulness of data processing. Article 4(11) of the GDPR defines consent as: *"*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"* Consent is presumed not to be freely given if the consent does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case. [60] Every new and different use of location data not covered under the introductory notice should provide separate notice to the users asking their consent. [61] For example, whenever location data become sensitive data, a separate and different user's consent should be obtained. Under EU law, article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The data subject must be informed of such a right prior to giving consent and he or she may exercise this right at his or her discretion. There can be no free consent if the data subject is unable to withdraw his or her consent without detriment or if withdrawal is not as easy as giving consent had been. [62] As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent remain lawful, however, the controller must stop the processing actions concerned. If there is no other

[59] F. Costantini, E Archetti, B Ferencz and F Di Ciommo, (2019) *Iot, intelligent transport systems and MaaS*, in https://cambiamo.net/publicaciones/iot-intelligent-transport-systems-and-maas-mobility-as-a-service/ Accessed August 2019, 5.

[60] P. Voigt, & A. Bussche, The EU General Data Protection Regulation (n. 46) 94.

[61] See again Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 38.*

[62] Handbook on European data protection law, (n. 39) 150.

lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller. [63]

5.3. Data Privacy Impact Assessment (DPIA)

MaaS provider is the owner of the technological platform where different datasets converge, and to which all customers address their demand. Among the many duties of this agent, two are worth mentioning because they are imposed in order to foster information security. [64] The first is the Data Protection Impact Assessment (DPIA) that has to be performed before starting the "processing" because MaaS can be defined as "*a systematic monitoring of a public accessible area on a large scale*" (Article 35. 3 (c) GDPR). The second is the obligation to notify a personal data breach to the supervisory authority within 72 hours (Article 33. 1 GDPR) and to the data subject "without undue delay" *ex* Article 34 .1 of the GDPR. Moreover, MaaS provider may be "*processing on a large scale of special categories of data referred to in Article 9(1)*" (Article 35. 3. (b) GDPR) or in *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling…* (Article 35. 3 (a) GDPR). Therefore, location data enforce the need of a DPIA on MaaS, having a central role in the above hypothesis because they are fundamental to monitor traveller's behaviours, they become sensitive in combination with other data and they could help MaaS provider to categorize its users.

DPIAs are important tools for accountability. [65] This new tool of the GDPR is highly relevant for any processing of personal data, as it helps to structure the process, be aware of data protection issues and the relevant legislation and implement proper safeguards to protect data subjects. DPIA begins before any data are processed and continues throughout the life cycle of a project and its data processing operations. At the heart of this process is the analysis of high risks to the rights and freedoms of individuals that may emanate from the processing of personal data and is the basis for mitigating these risks through technical and organisational measures. A DPIA must be undertaking by the controller who must first consider who will he ask to actually do the work of carry a DPIA on

[63] See Article 29 WP n. 259, 12/2017 (n. 56) 22.

[64] F. Costantini, MaaS and GDPR (n. 36) (2017).

[65] Article 29 WP n. 248, 4/ 2017 on guidelines on DPIA and determining whether data processing is likely to result in a high risk for the purpose of regulation 2016/679 https://ec.europa.eu /newsroom/article29/item-detail.cfm?item_id=611236. Accessed September 2019, 4.

his behalf. [66] If the DPIA finds that the risks to the rights of individuals remain high even with the identified measures, the controller has to consult the Supervisory Authority according to Article 36 GDPR before the processing can start. The controller may also decide to abandon the processing operation. It's clear that the GDPR requires a very broad analyse of the risk posed by a processing operation. The Article 29 of Data Protection Working Party on guidelines on DPIA suggest that there must be a consideration of all risks to rights and freedoms not just data protection rights. Whenever a controller concludes that the operation in question is not high risk it will want to retain a record of that assessment, so that it can demonstrate compliance with its obligation to consider article 35 GDPR. If the controller does not undertake a DPIA in circumstances where the Supervisory Authority concludes one should have been done then a fine up to 2 per cent of global turnover may be imposed (Art. 83 (4) (a) GDPR). If a DPIA has not been done then the Supervisory Authority could order than one be done in a specific manner and within a specific period (Art. 58 (2) (b). and it may limit or ban the controller from processing personal data in the meantime. (Art. 58 (2) (f) GDPR.) Moreover, data subjects may ask compensation for material or immaterial damage that they have suffered as a result of processing undertaken in the absence of a DPIA (Art. 82 GDPR).

5.4. Anonymization and Pseudonymization Location Privacy

In DPIA anonymisation techniques and pseudonymization could be considered as means of securing user identity. The WP 29 suggest that anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation while producing some useful data. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques. [67] In anonymised data, identifiable elements are irreversible destroyed in order to achieve irreversible deidentification of data subject. Pseudonymization substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject. With the advent of GDPR it is important to understand the difference between anonymized data

[66] D Kelleher, M Karen, *EU Data Protection Law* (n. 48) 269.

[67] Cfr Article 29 WP, Opinion 5/2014 n. 216 on Anonymization techniques https://www.dataprotection.ro/servlet/ViewDocument?id=1085 Accessed September 2019, 3

and pseudonymized data since the former are not considered as personal data. [68] In contrast, identifiable elements, are replaced by pseudonyms with which data subject cannot be directly identified, but identifiable data are reversible. The Working Party [69] (2014) emphasizes that there are two different approaches to anonymisation: the first is based on randomization while the second is based on generalization. Randomization is a family of techniques that alters the veracity of the data in order to remove the strong link between the data and the individual. If the data are sufficiently uncertain then they can no longer be referred to a specific individual. Randomization may protect against inference attacks/risks and can be combined with generalization techniques to provide stronger privacy guarantees. Otherwise, generalization consists of generalizing, or diluting, the attributes of data subjects by modifying the respective scale or order of magnitude (i.e. a region rather than a city, a month rather than a week).

Art. 4(5) GDPR introduce pseudonymization on a legal basis, which implies separating the identifying elements of personal data by pseudonyms. [70] Pseudonymization is mentioned as "an appropriate technical and organisational measures" for data protection and data minimization in Art. 25. (1) of the GDPR. For instance, obfuscation can be practical way for users to protect their location when engaging in LBSs. Instead of using their accurate location *x*, users employ a Location Privacy Protection Mechanism (LPPM) that computes a pseudo-location *z* and then transmits this pseudo-location to the service provider. As a result, the LBS provider and third parties receive only altered or approximate location instead of accurate location information. According to Herrmann [71] (2016), there are four main types of obfuscation strategies that have been extensively studied in the literature:

a) hiding location data: with this obfuscation strategy the user stops engaging in the LBS for a certain time or at a certain place;

b) perturbation: a user may perturb her location, i.e. use the library as her current location instead of her true location the hospital, in order to protect her location privacy;

c) reducing precision: instead of using accurate locations, the user provides

---

[68] Both scholars share the same position, P. Voigt, A. Bussche, *The EU General Data Protection Regulation* (n. 46) 13; S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 64.*

[69] Article 29 WP, Opinion 5/2014 n. 216 on Anonymization (66) 11.

[70] C Williamson, 'Pseudonymization vs anonymization and how they help with GDPR' in https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/ Accessed September 2019.

[71] M. Herrmann, 'Privacy' in Location Based Service (2016), in https://www.esat.kuleuven.be/cosic/publications/thesis-273.pdf Accessed August 2019, 55-63

a cloaking region to the LBS provider. For example, a user provides as location the region of a city instead of her accurate GPS coordinates;

d) and dummies: a dummy based LPPM queries the LBS with a series of fake locations that may include the user's actual location *x*. If the LBS accepts dummy queries, the LPPM can send the set of locations directly to the LBS and receives in return an answer to every location in *z*.

Another practical and safest way to protect location data is the recent practise adopted by Google [72] (2019) which now let's user to automatically delete location and activity history. However, latest research indicates that anonymization and pseudonymization are not sufficient at preserving the security of the data. An example that shows the potential of location data in de-anonymisation is the experiment conducted by De Montjoye. [73] They showed that with a dataset of location data they could uniquely identify 95% of the people in a large anonymised data set (approximately 1.5M users of a mobile phone operator). Confirming the previous Bettini's research [74] which showed that anonymization of location traces of a person is hardly possible because the traces of users are a spatiotemporal pattern that is almost unique to each user. Therefore, pseudo-anonymization does not offer any protection of user traces, because the pseudonym allows to reconstruct user traces.

6. Conclusions

Based on the value of location data, LBSs has risen. The importance of LBSs are undoubtful, however alongside the benefits, location data privacy vulnerabilities has been subject of concerns by scholars. As showed in section (5.1), on MaaS personal location data could become easily sensitive data in combination with other information. Processing data of the MaaS end-user and the improper use of sensitive data related to pattern trips are important legal concerns. Therefore, unlawful and unfair interference with location data has a direct nega-

[72] Mathew Katz (June 2019) Google will now let you auto-delete your location history, https://www.digitaltrends.com/android/google-automatically-delete-location-history/Accessed November 2019; See also, John Moreno (June 27, 2019) Google will now let you automatically delete location and activity history. Here's how https://www.forbes.com/sites/johanmoreno/2019/06/27/google-can-now-automatically-delete-your-location-data-heres-how/ Accessed November 2019

[73] Y.A. De Montjoye and others, *Unique in the Crowd: The privacy bounds of human mobility* (Scientific reports 2013) 1376.

[74] C. Bettini, C.X. Sean Wang, S. Jajodia, 'Protecting Privacy Against Location-Based Personal Identification' in *Second VLDB Workshop on Secure Data Management (SDM*, volume 3674 of *Lecture Notes in Computer Science* (Springer Berlin Heidelberg 2005) 185-199.

tive impact on privacy, which has a significant effect on the private lives of smartphone users and also of other individuals. In order to secure and protect the location data and privacy of smartphone users from unauthorised access, use, disclosure or retention, some administrative, regulatory and technical procedures are required. However, in such cases, and in many others, it seems that the guarantees provided by GDPR, either strictly legal (such as the consent of the data subject [Article 7 GDPR]), or technological (such as "Privacy by Design" [Article 25 GDPR]) are not suitable to avoid the risk that the "controller" or the "processor" could be punished accordingly. [75] Subsequently, bedside the guarantees and sanctions in case of data breach offered by GDPR, in order to fully protect personal location data privacy, more information and education about the risks, the values and opportunities emerging from personal data should be promoted by Supervision Authorities to the data subjects. In other words, a reciprocal cooperation will reduce the risk of unlawful and unfair processing of personal location data.

[75] F. Costantini and others, *Iot, intelligent transport systems and MaaS* (n. 58) (2019) 9.

SECTION II: COMMENTS ON DECISIONS

L'UTILIZZO DELL'ALGORITMO NELLE PROCEDURE VALUTATIVE DELLA PA (COMMENTO A CONSIGLIO DI STATO, SEZ. VI, SENT. 8 APRILE 2019, N. 2270)

Mariní Gaia Chiacchio

Abstract

Il Consiglio di Stato, con la sent. n. 2270/2019, si è pronunciato sull'utilizzo di un algoritmo all'interno di un procedimento concorsuale afferente all'assunzione di un gruppo di docenti.

In sintesi, il Supremo Consesso Amministrativo, superando quanto in passato sostenuto dalla Giurisprudenza, ha ritenuto legittimo, nonché preferibile, l'impiego dell'intelligenza artificiale all'interno di procedure seriali e standardizzate, prive di valutazioni di carattere discrezionale.

Gli strumenti digitali, invero, garantiscono maggior efficienza ed economicità all'*agere* amministrativo, in attuazione del principio costituzionale del buon andamento ex art. 97 cost..

Ciò nondimeno, l'algoritmo, in quanto atto amministrativo informatico, deve risultare conoscibile sia per le parti che per il giudice, corredando suddetta formula tecnica con spiegazioni idonee a tradurre il dato matematico in una regola giuridica.

Keyword: Atti e procedimenti amministrativi informatici, digitalizzazione della PA, intelligenza artificiale.

1. Enunciazione dei fatti

La Sesta Sezione del Consiglio di Stato, con sentenza n. 2270/2019, in riforma della pronuncia di primo grado, ha accolto il ricorso esperito da un gruppo di docenti avverso una procedura di assunzione [1], gestita interamente da un sistema informatico per mezzo di un algoritmo.

Più nel dettaglio, gli appellanti lamentavano che il meccanismo *de quo* fosse sfociato in provvedimenti irragionevoli, in quanto emanati senza tener conto delle preferenze indicate dalle parti, nonché privi di motivazione e in difetto di trasparenza.

Le parti, infatti, ignare delle concrete modalità di funzionamento dell'algoritmo, contestavano, altresì, l'assenza dell'individuazione di un funzionario deputato a valutare specificatamente le singole situazioni e a esternare correttamente le relative determinazioni provvedimentali.

2. Punti chiave e fondamenti giuridici

2.1. La digitalizzazione della Pubblica Amministrazione

Risulta da subito fondamentale specificare che l'utilizzo di un algoritmo all'interno di procedure di assunzione, prive del carattere della discrezionalità, si inserisce all'interno del fenomeno afferente la digitalizzazione della Pubblica Amministrazione (di seguito, "PA").

Punto di partenza indefettibile è l'art. 3 bis della l. 241/90, introdotto dall'art. 3 della legge n. 15 del 2005, alla luce del quale le amministrazioni, per conseguire maggiore efficienza alle attività cui sono preposte, devono incentivare l'uso della telematica, sia nei rapporti interni tra le diverse PPAA (attività c.d. di *back office*), che tra queste e i privati (c.d. *front office*) [2].

Parimenti, l'utilizzo delle tecnologie da parte della PA va necessariamente ricondotto al principio di trasparenza e di pubblicità *ex* art. 1, co. 1 della l. 241/90, in quanto sua diretta espressione.

Non a caso, nell'ultimo decennio, i siti *web* delle amministrazioni sono diventati il principale *front office* degli enti *de quibus*, garantendo, mediante una

[1] Con maggior impegno esplicativo, il caso in analisi concerneva una proposta di assunzione di docenti a tempo indeterminato, in conseguenza del piano straordinario nazionale di cui alla legge n. 107/2015 (art. 1 commi da 95 a 104).

[2] V.F. MARTINES, *La digitalizzazione della pubblica amministrazione*, in *Medialaws – Rivista dir. media*, II, 2018.

costante pubblicazione, l'accessibilità ai c.d. *open data* detenuti dalla PA, così come, peraltro, prescritto dal d.lgs. 33/2013.

A ben vedere, il fenomeno in analisi rappresenta indubbiamente un approdo fondamentale del diritto amministrativo, cui si è giunti in seguito a decenni in cui la funzione pubblica si connotava per i caratteri della segretezza e dell'oscurità, sia sotto il profilo dell'attività procedimentale che dell'organizzazione.

Orbene, nonostante già Mortati nel 1904 parlasse dell'amministrazione come una "casa di vetro", solo a partire dalla l. 241/90 il legislatore ha iniziato a comprendere che l'apertura della PA verso i cittadini è di fondamentale importanza [3], in quanto ha il precipuo compito di responsabilizzarla maggiormente, in un'ottica non solo giuridica, ma anche etica (c.d. *accountability*).

Il testo di riferimento principale in materia è rappresentato dal Codice dell'amministrazione digitale (c.d. "CAD") [4].

Quest'ultimo si configura come "una costituzione del mondo digitale", istituita per predisporre nuovi strumenti tecnologici, finalizzati a garantire l'espletamento di una PA che funzioni meglio e che, al contempo, costi meno ai cittadini.

In tal senso, basti pensare alle due figure innovative delineate all'interno dell'art. 17, come il responsabile per la transizione digitale e il difensore civico digitale unico a livello nazionale.

Più nello specifico, mentre al primo è attribuito il compito di riorganizzare gli uffici, "facendoli transitare alla modalità operativa digitale", il secondo, istituito presso la Agenzia per l'Italia Digitale (cd. "AgID2") [5], rappresenta un soggetto cui può rivolgersi "chiunque" per denunciare presunte violazioni del CAD da parte della PA [6].

Ciò nondimeno, risulta innegabile la valenza che le spinte sovrannazionali hanno assunto in tale ambito. Qui si inserisce la comunicazione del 26 settembre 2003 della Commissione Europea, la quale ha definito il c.d. *e-government* come "l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze, al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche" [7].

---

[3] V.M. SANTISE, *Coordinate ermeneutiche di diritto amministrativo*, Torino, 2018, 391 ss.

[4] D.lgs. 82/2005, modificato dal d.lgs. 179/2016 e dal d.lgs. 217/2017.

[5] Trattasi di un ente deputato a garantire l'attuazione da parte dell'amministrazione delle misure previste dal c.d. "piano triennale per l'informatica nella PA". Questo, invero, costituisce un documento fondamentale, non solo per l'organizzazione digitale, ma anche per gli investimenti in suddetto settore.

[6] Cfr. L. DELPINO-F. DEL GIUDICE, Manuale di diritto amministrativo, Napoli, 2019, 291 ss.

[7] V. F. BASSANINI, *Twenty years of administrative reforms in Italy,* in *Review of Economic*

2.2. La predilezione per gli strumenti digitali: le argomentazioni del Consiglio di Stato

Il giudice amministrativo, nell'argomentare le motivazioni afferenti il caso in analisi, parte da un dato fondamentale, sostenendo che "un più elevato livello di digitalizzazione dell'amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti."

In tale scia si pongono non solo il codice dell'amministrazione digitale, nonché i diversi interventi di riforma susseguitisi negli ultimi anni [8], ma, altresì, le spinte provenienti dall'ordinamento sovrannazionale.

Fondamentale è risultato essere, inoltre, il ruolo della dottrina, la quale ha elaborato il concetto di *e-government*, da intendere come processo di informatizzazione della PA, mediante l'utilizzo di modelli innovativi, incentrati sulle nuove tecnologie.

Ordunque, alla luce di tali premesse, l'utilizzo dell'algoritmo [9], all'interno di procedure seriali e standardizzate, non può che comportare indiscutibili vantaggi [10], purché non sia necessario l'esperimento di valutazioni di carattere discrezionale.

Pertanto, a detta dei giudici di Palazzo Spada, suddetto *modus operandi* deve essere incoraggiato, visti i numerosi benefici di carattere non solo economico, ma anche organizzativo.

Che sia così, risulta, peraltro, indirettamente deducibile da plurime disposizioni normative, come l'art. 1 della l. 241/90 [11], il quale inserisce all'interno dei

---

Conditions in Italy, 2009, III, 369 ss.; M. GASCÒ, *New Technologies and Institutional Change in Public Administration*, in *Social Science Computer Review*, 2003, I, 6 ss.

[8] L'ultimo rilevante intervento normativo sul punto è rinvenibile nella l. 124/2015.

[9] Questo viene definito dal Consiglio di Stato come "una sequenza ordinata di operazioni di calcolo che in via informatica sia in grado di valutare e graduare una moltitudine di domande".

[10] I giudici fanno, a titolo esemplificativo, riferimento alla "notevole riduzione della tempistica procedimentale", alla "esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario" e infine alla "maggior garanzia di imparzialità della decisione automatizzata".

[11] L'art. 1 della l. 241/90 recita: "1. L'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di imparzialità, di pubblicità e di trasparenza, secondo le modalità previste dalla presente legge e dalle altre disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario. 1-bis. La pubblica amministrazione, nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato salvo che la legge disponga diversamente. 1-ter. I soggetti privati preposti all'esercizio di attività amministrative assicurano il rispetto dei principi di cui al comma 1, con un livello di garanzia non inferiore a quello cui sono tenute le pubbliche amministrazioni in forza delle disposizioni di cui alla presente legge. 2. La pubblica amministrazione non può aggravare il procedimento se non per straordinarie e motivate esigenze imposte dallo svolgimento dell'istruttoria.

principi generali dell'attività amministrativa l'economicità e l'efficacia e l'art. 97 Cost. [12], relativo al principio di buon andamento.

Questi, invero, impongono alla PA l'esperimento della propria attività prediligendo procedimenti più snelli e accelerati.

3. Decisione finale

3.1. La soluzione adottata dal Consiglio di Stato

I giudici di Palazzo Spada, delineate le argomentazioni sopraesposte, volte a privilegiare l'utilizzo di modelli tecnologici e informatici, si soffermano sulla valenza giuridica dell'algoritmo all'interno di procedure standardizzate.

L'utilizzo di procedimenti "robotizzati", a ben vedere, non può costituire un *escamotage* per derogare alle norme afferenti lo svolgimento dell'attività amministrativa.

Pertanto, l'algoritmo, in quanto atto amministrativo informatico a tutti gli effetti, deve sottostare alle disposizioni concernenti l'agire pubblico, quali i principi di trasparenza e pubblicità.

Questo, dunque, deve risultare conoscibile non solo per i soggetti interessati, ma, altresì, per il giudice, corredando suddetta formula tecnica con spiegazioni capaci di tradurla in una regola giuridica.

Purtuttavia, non essendo ancora possibile sovrapporre l'intelligenza artificiale a quella umana, non può essere demandata al *software* alcuna valutazione di tipo discrezionale.

Alla luce di tali considerazioni, l'appello, per i giudici amministrativi, deve in questo caso trovare accoglimento per due ordini di motivi.

In primo luogo, per la violazione del principio di trasparenza, non essendo stata messe le parti nella condizione di comprendere e tradurre il *modus operandi* dell'amministrazione, attraverso il quale sono stati assegnati i posti disponibili.

In secondo luogo, alla luce della lesione del canone di ragionevolezza, essendosi verificate situazioni paradossali che hanno visto docenti con svariati anni di servizio assegnati a sedi mai richieste, nonché situate a centinaia di chilometri

[12] L'art. 97 della Costituzione dispone che: "I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione. Nell'ordinamento degli uffici sono determinate le sfere di competenza, le attribuzioni e le responsabilità proprie dei funzionari. Agli impieghi nelle pubbliche amministrazioni si accede mediante concorso, salvo i casi stabiliti dalla legge".

di distanza dalla propria residenza, mentre altri docenti, con minor esperienza, hanno, al contrario, ottenuto le sedi da loro richieste.

3.2. Osservazioni conclusive

La pronuncia in analisi rappresenta un ulteriore significativo contributo giurisprudenziale, teso a incentivare l'utilizzo di strumenti informatici ed elettronici all'interno dell'attività della PA.

A ben vedere, a differenza di quanto in passato affermato dal TAR Lazio, con la sentenza n. 9227/2018, in riferimento ad una fattispecie similare, in cui i giudici avevano sostenuto la necessità di un apporto "umano" al procedimento amministrativo [13], il Consiglio di Stato si è pronunciato a favore dell'utilizzo dell'intelligenza artificiale all'interno di procedure c.d. "standardizzate", ciò nondimeno, individuando diverse cautele.

Invero, i giudici di Palazzo Spada, nel caso *de quo*, hanno ritenuto illegittimo il procedimento, ma non perché l'intervento umano deve essere considerato essenziale, così come sostenuto dal TAR Lazio, ma poiché l'algoritmo, in quanto atto amministrativo informatico, deve sottostare ai principi di trasparenza e di ragionevolezza [14].

Una soluzione contraria, infatti, si porrebbe in contrasto con la *ratio* primaria del processo di digitalizzazione della PA. Tale riforma, invero, è nata col principale obiettivo di velocizzare e di snellire la macchina pubblica, rendendola, peraltro, più trasparente e favorendo, in tal modo, il dialogo e la collaborazione con il singolo cittadino [15].

Va sottolineato, infine, l'apporto indispensabile della giurisprudenza, evincibile, altresì, in suddetta sentenza, nell'adattare fattispecie concrete, afferenti il mondo delle nuove tecnologie, alle disposizioni legislative. Grazie ad una costante attività ermeneutica, infatti, i giudici riescono a plasmare lo statico dato normativo a delle figure giuridiche di nuovo conio, garantendo, in tal modo una legalità di tipo sostanziale.

---

[13] V. Redazione, *Atti e procedimenti amministrativi informatici: promossa la P.A. Robot, se l'algoritmo è conoscibile* in www.giurdanella.it, 29.4.2019.

[14] Tali principi sembrano echeggiare la scelta legislativa compiuta a livello europeo con il Reg. (UE) 679/2016, in cui ragionevolezza e trasparenza sono posti a presidio dei diritti e delle libertà degli individui coinvolti in "processi decisionali automatizzati" (artt. 21 e 22). Invero, al generale principio di trasparenza (corredato dal diritto di essere informati *ex* artt. 11, 12 e 13 del Regolamento), agli individui vengono, altresì, riconosciuti il diritto a ottenere l'intervento umano, ad esprimere la propria opinione, ovvero a contestare la decisione automatizzata.

[15] Per un approfondimento sul punto, G. SANTO, *La digitalizzazione del procedimento amministrativo*, 2018, Lecce.

D'altronde, in un contesto applicativo in continua evoluzione, quale quello afferente la digitalizzazione della PA, le disposizioni legislative possono spesso risultare obsolete, nonché difficili da adattare ai più recenti sviluppi tecnologici.

Legislazione rilevante

1. Codice dell'amministrazione digitale, d.lgs. 82/2005, modificato dal d.lgs. 179/2016 e dal d.lgs. 217/2017.
2. Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazione da parte delle pubbliche amministrazioni, d.lgs. 14 marzo 2013, n. 33.
3. Regolamento (UE) 2016/679, d.lgs. 193/2016.

LA BANCA NON PUÒ BLOCCARE L'OPERATIVITÀ DEL CLIENTE SE QUESTI NON FIRMA L'AUTORIZZAZIONE AL TRATTAMENTO DEI DATI (COMMENTO A CASS. CIV., SEZ. I, ORD. 21 OTTOBRE 2019, N. 26778)

Mario Triggiani

Abstract

La Corte di Cassazione, con l'ordinanza n. 26778/2019, ha dichiarato la nullità la clausola del contratto di conto corrente con cui la banca aveva subordinato l'esecuzione delle operazioni richieste dal cliente al rilascio del consenso al trattamento dei dati sensibili. In particolare, la Cassazione ha sancito che la banca non può bloccare l'operatività del cliente se questi non firma l'autorizzazione al trattamento dei dati sensibili, precisando che la condotta della banca comporta la responsabilità della stessa per inadempimento contrattuale, in quanto la richiesta del consenso è da intendersi come contraria a norme imperative dato che la legge sulla privacy ha natura di norma imperativa, contenendo precetti che non possono essere derogati dall'autonomia privata.

Keyword: dati personali; dati sensibili; autonomia contrattuale.

Summary: Introduzione. – 1. Il fatto. – 2. Le considerazioni della Corte. – 3. Le conclusioni.

Introduzione

Lo scorso 21 ottobre la I Sezione Civile della Corte di Cassazione ha affrontato con ordinanza n.26778/2019 la questione della legittimità del blocco da parte della banca dell'operatività del conto corrente bancario e del deposito titoli di un cliente che abbia rifiutato di sottoscrivere l'autorizzazione al trattamento dei propri dati sensibili, cioè idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati associazioni od organizzazioni a carattere religioso nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. [1]

[1] Definizione fornita dall'art.4 della versione previgente del d.lgs. 196/2003, articolo abro-

1. Il fatto

Nel caso di specie la Deutsche Bank s.p.a. aveva provveduto a bloccare dai primi giorni del 2008 le operazioni del proprio cliente E.L. in quanto quest'ultimo non aveva autorizzato la banca al trattamento dei suoi dati sensibili nonostante fosse stato avvisato che tale rifiuto avrebbe comportato l'impossibilità di dar corso alle operazioni richieste dal correntista.

Proprio l'informazione fornita al cliente circa la necessarietà dell'acquisizione da parte della banca dei suoi dati sensibili era stata posta alla base delle decisioni del giudice di primo e di secondo grado, che avevano ritenuto che il comportamento della banca non configurasse violazione della legge sulla privacy o inadempimento contrattuale.

2. Le considerazioni della Corte

La Corte di Cassazione ha, invece, accolto il ricorso del correntista evidenziando come, già sulla base della normativa previgente (applicabile al caso di specie) l'autonomia contrattuale non possa porsi in contrasto con norme imperative come il codice privacy (d.lgs. 196/2003), il cui art. 23 comma 3 (versione previgente [2]) sancisce che il consenso al trattamento dei dati personali debba essere prestato liberamente, e quindi certamente non sotto le pressioni di una minaccia di bloccare conto corrente e deposito titoli.

D'altro canto tale legge consente il trattamento dei dati personali (ed a maggior ragione di quelli sensibili) solo qualora questi siano indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati.

Il Collegio osserva come non risultava, nel caso di specie, che la banca avesse spiegato concretamente la necessità del trattamento dei dati sensibili, avendo semplicemente affermato che per propria policy aziendale fossero utili per un miglior rapporto con la clientela.

Non essendovi dunque alcun reale bisogno per la banca di trattare i dati sensibili, questi si configurano come non pertinenti e non indispensabili.

Se è teoricamente ipotizzabile che la banca possa trovarsi in possesso di dati sensibili dei clienti e che si trovi in necessità di avere un consenso per poterli

gato dal d.lgs. 101/2018 che ha adeguato la normativa nazionale al Regolamento UE 2016/679.

[2] *Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo.*

distruggere, la Cassazione ha ribadito che non è questo motivo sufficiente per obbligare i correntisti a fornire il consenso al trattamento (nozione che comprende una quantità di operazioni che vanno ben oltre la mera distruzione) dei dati in luogo di un mero consenso una tantum alla cancellazione degli stessi qualora raccolti incidentalmente.

3. Le conclusioni

La condotta della banca che blocca l'operatività del conto corrente bancario e del deposito titoli del correntista il quale non abbia sottoscritto l'autorizzazione al trattamento dei dati sensibili integra dunque responsabilità della stessa per inadempimento contrattuale in quanto la richiesta del consenso è da intendersi come contraria a norme imperative.

Il Regolamento, pur non richiamando mai espressamente la nozione di "dato sensibile" sancisce all'art. 9 che "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*" indicando successivamente i casi tassativi in cui non si applica tale disposizione.

NON SERVE IL CONSENSO DEI PROPRIETARI DELLA VILLA PER LA PUBBLICAZIONE DI FOTO DA PARTE DELL'IMPRESA CHE HA RIFATTO GLI INFISSI (COMMENTO A CASS. CIV., SEZ. III, ORD. 29 OTTOBRE 2019, N. 27613)

Mario Triggiani

Abstract

La Corte di Cassazione, con l'ordinanza n. 27613/2019, ha sancito che non è configurabile la responsabilità da violazione del diritto alla privacy, all'immagine o della proprietà altrui nel comportamento di chi acquisisca dati contenenti immagini della propria opera, pubblicandoli sul proprio catalogo nel proprio personale interesse. Tuttavia, le fotografie scattate dal prestatore d'opera e pubblicate senza consenso dei committenti devono essere prive di qualsivoglia riferimento alla vita privata, ai beni personali o al lavoro dei committenti.

Keyword: diritto alla privacy; diritto all'immagine; diritto di proprietà.

Summary: Introduzione. – 1. Il fatto. – 2. Le considerazioni della Corte.

Introduzione

Con ordinanza n.27613/2019 la III Sezione Civile della Corte di Cassazione ha affrontato lo scorso 29 ottobre la questione della necessità del consenso dei proprietari di un immobile affinché l'impresa che abbia effettuato lavori di rifacimento degli infissi dello stesso possa pubblicizzare le foto del lavoro effettuato all'interno del proprio catalogo pubblicitario.

1. Il fatto

È quanto accaduto nel caso dei coniugi B.R. e C.E., proprietari di una villa,

che hanno spiegato ricorso contro il provvedimento adottato dal giudice di secondo grado, il quale aveva rigettato la domanda di risarcimento del danno non patrimoniale nei confronti dell'impresa SIALWOOD S.r.l., per aver pubblicato, nel proprio catalogo pubblicitario, le immagini dei manufatti effettuati nei lavori di rifacimento degli infissi della suddetta villa.

I coniugi lamentavano che la mancata prestazione del loro consenso alla pubblicazione delle immagini dell'interno della propria abitazione privata configurasse una violazione degli obblighi contrattuali propri del prestatore d'opera.

Il prestatore d'opera deve infatti comportarsi secondo le regole di correttezza e buona fede, considerate dai coniugi incompatibili con il comportamento di chi, avendo avuto accesso ad un'abitazione privata, abbia successivamente utilizzato le immagini scattate all'interno della dimora per scopi promozionali violando di conseguenza il diritto alla privacy ed all'immagine dei committenti, che vedevano di fatto pubblicati i propri dati personali.

2. Le considerazioni della Corte

La Corte di Cassazione ha rigettato la domanda affermando che può parlarsi di violazione degli obblighi di salvaguardia dell'interesse del committente solo qualora dalle immagini scattate dal prestatore d'opera e pubblicate senza consenso dei committenti possa desumersi un qualsivoglia riferimento alla vita privata, ai beni personali o al lavoro dei committenti.

Non può dirsi invece violato il diritto alla privacy qualora le immagini presentino, come nel caso di specie, un carattere di "neutralità". Le foto scattate dall'impresa, infatti, si limitavano a documentare le caratteristiche estetiche e tecniche del manufatto eseguito dal prestatore d'opera.

La Corte ha infatti anche chiarito che al prestatore d'opera deve essere sempre garantita la possibilità di acquisire immagini del proprio manufatto, anche se riferite a parte del mobilio o degli ambienti in cui esso si inserisce, senza che sia necessario il consenso del committente alla pubblicazione delle foto.

Ciò che rileva ai fini della compatibilità degli scatti pubblicitari con il diritto alla privacy è che le immagini si dimostrino prive di qualsivoglia contenuto personale riferito al committente dell'opera.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA WELTIMMO, C-230/14 ECLI:EU:C:2015:639

Adrián Palma Ortigosa

Abstract:

Una sociedad domiciliada en Eslovaquia gestiona una página web de anuncios de inmuebles situados en Hungría. Algunos anunciantes de dicho web, tras pasar el periodo gratuito de publicación de dichos inmuebles, solicitaron la retirada de sus anuncios, sin embargo, dicha sociedad se negó a tal retirada y le facturó tales servicios en los meses sucesivos, meses que no fueron pagados por tales anunciantes, lo que llevo a la empresa a transmitir dichos datos de los anunciantes en cuestión a empresas de cobro de impagados. (Cesión de créditos). Los anunciantes denuncian ante la autoridad de control húngara tal tratamiento de datos. Dicha autoridad sanciona a esta empresa, lo que lleva a esta última a recurrir tal sanción señalando que la autoridad húngara no tiene competencia, sino que debería de ser en su caso la autoridad eslovaca (país donde está domiciliada la empresa) la competente para conocer del asunto. (FJ 9 a 13).

Cuestiones claves del asunto:

A) Normativa aplicable:

El TJUE en primer lugar analiza cual debería de ser la normativa que debería de aplicarse en materia de protección de datos al responsable del tratamiento (empresa eslovaca). Esto es, la Ley eslovaca o bien la Ley húngara. En este sentido, el TJUE llega a la conclusión de que la autoridad de control podrá aplicar la normativa húngara ya que a efectos del Art 4.1 a) de la Directiva 95/46, el tratamiento de datos se ha efectuado en el marco de las actividades de un establecimiento en el territorio de Hungría (FJ 39). Ya que, la susodicha empresa ejerce una actividad real y efectiva en Hungría. (FJ 32), siendo mínima, pero estable (FJ 31). Y ello es debido a que dicha empresa gestiona varios sitios de Internet de anuncios de inmuebles situados en Hungría y estos anuncios están redactados en húngaro (FJ 32) Además, la referida sociedad abrió una cuenta bancaria en Hungría, así como un apartado de correos en Hungría. (FJ 33). Siendo además dicho tratamiento de datos efectuado en el marco de actividades anteriormente descritas. (FJ 38)

B) Potestades de Autoridad de Control respecto de otro EEMM:

El TJUE, en relación a una de las cuestiones prejudiciales que le plantean, viene a tratar cuales serían las facultades y potestades que ostentaría la autoridad de control cuando la ley aplicable al responsable del tratamiento fuera la de otro estado miembro por entender que la susodicha empresa no ostenta un establecimiento en Hungría sino en Eslovaquia. En estos casos, el TJUE considera, que si bien, la autoridad de control tendría potestad para realizar potestades de investigación, consultas etc (FJ 54), más allá de ello, no podría establecer sanciones fuera de su territorio (FJ 59), lo que llevaría a dicha autoridad húngara a solicitar a la autoridad eslovaca la cooperación en esta materia. (FJ 58).

Decisión Final: El artículo 4.1 a) de la Directiva 95/46 permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que este último ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento. (FJ 66.1).

En el supuesto de que la autoridad de control de un Estado miembro que conoce de unas denuncias, llegue a la conclusión de que el Derecho aplicable al tratamiento de los datos personales de que se trata no es el Derecho de ese Estado miembro, sino el de otro Estado miembro, dicha autoridad de control sólo podría ejercer en el territorio de su propio Estado miembro determinadas facultades que nunca podrán comprender la imposición de sanciones basadas en el Derecho de ese estado miembro del responsable del tratamiento de tales datos, debiendo instar a la autoridad de control del Estado miembro en cuestión que inicie las correspondientes actuaciones. (FJ 66.2).

Artículos implicados del REPD: Arts. 55 a 62.

Apartado concreto del Temario: 1.10.1 y 1.10.2.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA SCHREMS. ASUNTO C-362/14. ECLI: EU:C:2015:650

Adrián Palma Ortigosa

Abstract:

Ciudadano Irlandés denuncia la Decisión 2000/520 acordada por la Comisión Europea referida al acuerdo de puerto seguro entre la Comisión y EEUU. Dicha decisión está basada en lo previsto en el Art 25.6 de la Directiva 95/46/CE que permite la realización de acuerdos entre la Comisión Europea y terceros países. En estos acuerdos se certifica que terceros países presentan un nivel de protección adecuado en el tratamiento de los datos personales, permitiéndose así que se puedan transferir datos personales provenientes de Europa a dichos países. Este ciudadano denuncia que Facebook transfiere los datos de su perfil a EEUU basada en dicha Decisión 2000/520, indicando que dicho país no satisface las exigencias que garantizan un nivel adecuado de cumplimiento de la normativa europea de protección de datos.

Cuestiones claves del asunto:

A) Funciones de las autoridades de control en relación a las transferencias de datos internacionales en caso de existir un acuerdo de puerto seguro entre la Comisión y Tercer Estado

Aunque exista un acuerdo de puerto seguro vía Decisión de la UE-Tercer Estado, el TJUE considera que una Autoridad de Control, si bien no puede declarar la invalidez de dicha decisión, si está legitimada para examinar la solicitud de una persona que alega que el Derecho y las prácticas en vigor de ese tercer estado no garantizan un nivel de protección adecuado. Pudiendo en su caso el interesado acudir a los órganos jurisdiccionales cuando las autoridades de control les nieguen sus peticiones. (FJ 64, 65 y 66).

Si la legislación no permitiera que una autoridad de control revise una solicitud de un particular, dicha previsión sería contrario al sistema establecido por la Directiva 95/46 (FJ 56), quedando privados dichos titulares del derecho garantizado por el artículo 8, apartados 1 y 3, de la CDFUE. (FJ 58).

Por tanto, una autoridad de control está legitimada para revisar una solicitud de un interesado que pone en cuestión una Decisión de la Comisión aprobando un acuerdo de transferencia internacional de datos personales. Pudiendo en su caso acudir a los tribunales para exigir sus derechos.

B) Transferencia de datos transfronterizos a terceros estados. Acreditación de un nivel adecuado de protección por parte de un tercer estado

Significado del término ***"adecuado"***. Si bien, no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión Europea. Sin embargo, si es exigible que ese tercer país garantice efectivamente por su legislación interna o sus compromisos internacionales un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión. (FJ 73).

Entre los aspectos que han de valorarse para considerar que un país cumple con un nivel adecuado de protección se han de tener en cuenta: (FJ 75).

- El contenido de las reglas aplicables en ese país derivadas de la legislación interna o de los compromisos internacionales de éste.
- La práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país.
- Por otro lado, dado que ese nivel puede variar, cuando existan indicios fundados, se deberá de actualizar dicho cumplimiento.

En este caso, el TJUE considera que no se cumple tal adecuación, ya que:

- Los principios de puerto seguro establecidos en la Decisión de la Comisión Europea no se exigen a las autoridades públicas estadounidenses. FJ 82
- Además, las autoridades públicas pueden acceder a los datos personales de los ciudadanos europeos sin limitación alguna en virtud de una excepción de carácter general relativa a principios tales como: las exigencias de seguridad nacional, interés público y cumplimiento de la ley. FJ 87.
- La Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar posibles injerencias (FJ 88) y tampoco pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza (FJ 89).

Decisión Final: EL TJUE declara la invalidez de la Decisión 2000/520/CE de la Comisión Europea adoptada al quedar acreditado que la normativa de EEUU no garantiza un nivel adecuado de protección de los derechos fundamentales sustancialmente equivalente al garantizado por el ordenamiento jurídico de la UE. FJo67 y FJo 89. Ya que, una normativa que autoriza de forma generali-

zada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización (FJ 93), excede de los estrictamente necesario de una medida limitadora de derechos. (FJ 91 Y 92).

Artículos implicados del REPD: Art 45, Considerando 104, Considerando 106.

Apartado concreto del Temario: 1.9, 1.9.1, 1.9.2.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA COMISIÓN/HUNGRÍA, C-288/12, ECLI:EU:C:2014:237

Adrián Palma Ortigosa

Abstract:

El Sr. Jóri fue nombrado Supervisor de protección de datos de Hungría el 29 de septiembre de 2008. Su cargo debía de extenderse durante 6 años, sin embargo, el 31 de diciembre de 2011 este fue cesado debido a la entrada en vigor de una nueva legislación establecida por el nuevo gobierno que entró en el poder. La Comisión Europea impugna tal decisión.

Cuestiones claves del asunto:

A) Mandatos de la autoridad de control: (Independencia)

Partiendo de que el principio de independencia de las Autoridades de Control es sustancial dicho cargo. (FJ 51 Y 52), toda medida por la cual un Estado Miembro pueda limitar el cargo previamente establecido sin apoyo legal justificado, puede generar un efecto de obediencia anticipada en las autoridades de control, quedando en entredicho dicho principio de independencia por parte de las autoridades de control. (FJ 53 Y 54).

Decisión Final:

De lo anterior se desprende que Hungría puso fin al mandato del Supervisor sin respetar las garantías establecidas por la ley para proteger su mandato, menoscabando de este modo su independencia en el sentido del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 (FJ59).

Artículos implicados del REPD: Considerando 117, 118, Art 51, 52, 53 y. 54.

Apartado concreto del Temario: 1.10.1.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIAS DIGITAL RIGHTS IRELAND Y SEITLINGER Y OTROS , C-293/12 Y C-594/12, ECLI:EU:C:2014:238

Adrián Palma Ortigosa

Abstract:

En el presente asunto una entidad denominada Digital Rights considera que la la Directiva 2006/24 es nula debido a que esta normativa impone a los proveedores de servicios de comunicación telefónica la obligación de conservar los datos de tráfico y localización relativos a las comunicaciones que estas empresas controlan. En este sentido, la Directiva establece como justificación para la conservación de tales datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves.

Se duda por tanto de la legalidad de la medida a través de la cual esos proveedores y en base a las exigencias de las autoridades, deben de conservar los datos durante un determinado periodo de tiempo y pueden acceder a un sinfín de datos personales de gran cantidad de personas.

Cuestiones claves del asunto:

A) Vulneración Art 8 CDFUE. Carácter necesario del uso del tratamiento de datos:

Para valorar la posible nulidad de la Directiva por vulneración del derecho a la protección de datos, el TJUE parte de la premisa de considerar que una regulación como la establecida por la Directiva 2006/24 es como tal una injerencia a dicho derecho fundamental (FJ 33). Ello es así porque en dicho texto legal se regula el tratamiento de datos de carácter personal (FJ 34), ya que los proveedores de servicios deben de conservar durante un tiempo determinado gran cantidad de datos personales.(FJ 36) Ahora bien, si bien es cierto que dicha injerencia ha de considerarse de gran magnitud y especialmente grave (FJ 37), se ha de valorar si dicha injerencia cumple con las exigencias previstas en la CDFUE que permitirían una limitación al derecho a la protección de datos contenido en la Carta. Habida cuenta de ello, se habrá de valorar si dicha limitación del derecho a la protección de datos respeta; su contenido esencia, el principio de pro-

porcionalidad, y además, dicha medida analizada es necesaria y responde a un objetivo de interés general (FJ 38).

Pues bien, por lo que se ***refiere al contenido esencial*** y al hecho de valorar si dicha injerencia responde a un ***objetivo de interés general***. El TJUE llega a la conclusión de que no se produce tal vulneración del contenido esencial en la medida que la propia normativa prevé reglas que tienen en consideración la protección de datos (FJ 40), además, el objetivo de interés general está justificado debido a que con esta Directiva se contribuye a la lucha contra la delincuencia grave y, en definitiva, a la seguridad pública. (FJ 41). (objetivos de interés general.

En relación a ***la proporcionalidad*** de la injerencia constatada, dado que esta Directiva supone una injerencia grave al derecho fundamental a la protección de datos, la facultad de apreciación del legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto (FJ 48). Así, por lo que se refiere a la cuestión de si la conservación de datos ***es adecuada*** para lograr el objetivo perseguido por la Directiva 2006/24, el TJUE considera que la Directiva puede ser una herramienta útil para las investigaciones penales. (FJ 49).

En cuanto al ***carácter necesario*** de la conservación de datos, si bien el TJUE entiende que la lucha contra el terrorismo reviste una importancia primordial para garantizar la seguridad pública y su eficacia depende en gran medida de la utilización de técnicas modernas de investigación. Este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha. (FJ 51). En este sentido, la normativa que regule las injerencias de estos derechos ha de establecer reglas claras y precisas (FJ 54). Sin embargo, esta Directiva es aplicable a todos los medios electrónicos, comprendiendo así a todos los abonados y usuarios que usen tales medios, afectando por tanto a prácticamente toda la población europea. (FJ 56), todo ello, sin que se establezca ningún tipo de diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves. (FJ 57 Y 58). Además, tampoco se fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención de delitos (FJ 60).Por último, tampoco se garantiza la destrucción definitiva de los datos al término de su período de conservación. (FJ 67) y el control de estos dentro del territorio de la Unión. (FJ 68).

Decisión Final: El TJUE considera que la Directiva 2006/24 es inválida conforme a los términos descritos en el párrafo anterior. (FJ 71).

Artículos implicados del REPD: Se analiza la Directiva 2006/24/CE. (Actualmente Directiva 2016/136.

No obstante, puede relacionarse con los Art 5.1 c) (Minimización de datos) Art 5.1 b) (Limitación de datos).

Apartado concreto del Temario: 1.14.3 Puede relacionarse con: 1.3.5 y 1.3.4.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA. FRANTIŠEK RYNEŠ, C-212/13, ECLI:EU:C:2014:2428

Adrián Palma Ortigosa

Abstract:

Un ciudadano instala varias cámaras de video-vigilancia en su vivienda. En una de las ocasiones, esas cámaras captaron a varias personas causando desperfectos en la vivienda de dicho ciudadano, tales grabaciones fueron utilizadas a la hora de iniciar las correspondientes investigaciones penales, sirviendo además como prueba a la hora de imponer las sanciones que la norma prevé al efecto. Los sospechosos denuncian ante la Agencia de Protección de Datos la legalidad de dicho sistema de Video vigilancia. En este sentido, la Agencia de Protección de Datos checa considera que el titular de las cámaras, como responsable del tratamiento de datos, ha incumplido la normativa en materia de protección de datos.

Cuestiones claves del asunto:

A) Concepto de datos Personales. Grabación de imágenes por video cámara

Por lo que se refiere a la captación de imágenes por parte de una cámara de video vigilancia, el TJUE llega a la conclusión que dicha captación de imágenes constituye un dato personal a efectos de la Directiva. (FJ 22).

B) Tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas

Para valorar si el tratamiento de datos que lleva a cabo el titular de la vivienda queda fuera del ámbito de aplicación de la Directiva 95/46 por considerar que estamos ante la llamada excepción doméstica, el TJUE, en primer lugar llega a la conclusión de que el tratamiento de datos que lleva a cabo el titular de las cámaras (responsable), es un tratamiento a efectos de la directiva 95/46. (FJ25). Sentadaestapremisa,elTJUEpasaavalorarsilacaptacióndeimágenesmediantevideo cámara puede estar exceptuada del ámbito de aplicación de la directiva

por considerar que nos encontramos ante un tratamiento que se realiza en el ejercicio de actividades exclusivamente personales o domésticas. Art 3.2 Directiva 95/46.

Así, el TJUE entiende que, dado que parte de la captación de imágenes abarca el espacio público, el tratamiento de datos personales en estos casos no puede considerarse una actividad exclusivamente personal o doméstica, ya que esta excede de la esfera propiamente privada de la persona de la que procede el tratamiento de datos.

Decisión Final:

La captación de imágenes mediante video cámara supone un tratamiento de datos conforme a la Directiva de protección de datos, además, dado que dicha captación de imágenes es realiza en parte hacia la vía pública, dicho tratamiento de datos ha de cumplir las exigencias legales de la Directiva 95/46. Es por ello, que no nos encontramos ante un supuesto de exclusión de aplicación de la Directiva derivada de la excepción doméstica prevista por la Directiva.

Artículos implicados del REPD: Considerando 18, Art 2.1.c).

Apartado concreto del Temario: Art 1.2.1. Ámbito de aplicación material.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA - GOOGLE SPAIN Y GOOGLE, C-131/12, ECLI:EU:C:2014:317

Adrián Palma Ortigosa

Abstract:

Un ciudadano (Señor Costeja) presentó una reclamación ante la AEPD para que esta última y de acuerdo a sus potestades:
A) Obligara al periódico La Vanguardia a eliminar o en su caso modificar una publicación que aparecía en dicho diario sobre este ciudadano.
B) Exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales con el objetivo de que dichos datos dejaran de incluirse en sus resultados de búsqueda y no pudieran vincularse a los enlaces de La Vanguardia.
La AEPD en su resolución no admitió la petición del Señor Costeja respecto al periódico la Vanguardia, pero sí en cambio en relación a Google Spain. De esta manera, la AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puedan lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona. Esta resolución fue recurrida por parte de Google ante la Audiencia Nacional siendo este último órgano judicial el que plantea la cuestión prejudicial ante el TJUE.

Cuestiones claves del asunto:

A) Tratamiento de datos. Moto de búsqueda

La actividad llevada a cabo por los motores de búsqueda ha de ser considerada como tratamiento de datos conforme a la Directiva 95/46. (FJo 27 y 28).

B) Responsable. Motor de búsqueda

El gestor del motor de búsqueda es quién determina los fines y los medios de esta actividad y, además, es el que lleva a cabo el tratamiento de datos personales, por consiguiente, debe considerarse responsable a efectos de la Directiva 95/46. (FJ 33). Es una interpretación amplia de la definición de responsable que trata de garantizar el pleno respeto de los derechos fundamentales. FJ 34. Por

tanto, el TJUE considera que Google Inc, como gestor del motor de búsqueda (Google Search) es considerado responsable a efectos de la Directiva.

C) Ámbito territorial. Concepto "Dentro del Marco de las actividades"

Pues bien, una vez que el TJUE considera que Google Inc es responsable.

Se procede a valorar si la Directiva le sería de aplicación a dicho responsable aunque no se encuentre situado en la UE, pero si ostente una filial en España (Google Spain)

Para ello, el TJUE se remite a lo contenido en el Art 4.1 a) y analiza el concepto de establecimiento a efectos de aplicar esta Directiva en los casos en los que en un responsable este situado fuera de la UE. En este sentido, dicho artículo prevé la aplicación de la Directiva a todo tratamiento de datos personales cuando:

El tratamiento sea efectuado ***en el marco de las actividades de un establecimiento*** *del responsable del tratamiento en el territorio del Estado Miembro...*

Para ello, en primer lugar analiza el concepto de establecimiento y se ayuda de lo contenido en el Considerando 19 de la Directiva. En este sentido, el TJUE llega a la conclusión de que Google Spain ha de considerarse un establecimiento a efectos de dicho precepto ya que esta última entidad se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. De esta manera, una vez que Google Spain es considerado un establecimiento de Google Inc, faltaría analizar si el tratamiento que lleva a cabo el responsable (Google Inc.) se realiza en el ***marco de las actividades*** de un establecimiento del responsable del tratamiento.

Así, el TJUE viene a entender que el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa en el *marco de las actividades* de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor. (FJ 55).

Y ello es así, ya que Google Spain es una filial de Google Inc. en territorio español, y, por lo tanto, un «establecimiento» en el sentido del artículo 4.1 a) de la Directiva 95/46, sin que dicho precepto exija que el tratamiento de datos personales controvertido sea efectuado por el propio establecimiento en cuestión, sino que basta con que se realice en el marco de las actividades de éste. FJ 52. Esta interpretación del Art 4.1 a) pretende evitar que una persona se vea excluida de la protección garantizada por la Directiva, estableciéndose un ámbito de aplicación territorial particularmente extenso. (FJ 53 Y 54).

D) Cancelación de datos por parte del motor de búsqueda

El TJUE, basado en los Art 12. b) y Art 14.a) (Derecho de supresión y Derecho de oposición respectivamente) analiza si los interesados tienen derecho a que se elimine de la lista de resultados de los motores de búsqueda toda información que aparezca sobre ellos una vez que se introduce el nombre de los interesados en dichos buscadores, incluso, en aquellos casos en los que dicha información sea lícita.

Así, el TJUE considera que el tratamiento de datos personales que llevan a cabo los motores de búsqueda supone una grave injerencia para los derechos fundamentales del respeto a la vida privada y el derecho a la protección de datos de los interesados *toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate* (FJ 80).

Por tanto, debido a la gravedad de dicha injerencia, la mera alegación del interés económico del gestor del motor de búsqueda no puede justificar como tal, dicho tratamiento. Así, a la hora de ponderar el ejercicio de los derechos de supresión y oposición en la materia analizada se ha de tener en cuenta los intereses legítimos que ostentan los internautas a la hora de poder acceder al contenido de la información referida al interesado. En este sentido, aunque en un principio el derecho a la protección de datos y el derecho la intimidad del interesado prevalecería respecto del derecho de los internautas a obtener dicha información, habrá no obstante que ponderar cada caso en relación a distintas variantes. (FJ 81).

E) Derecho al olvido

El TJUE analiza la última cuestión prejudicial que le plantea el órgano jurisdiccional nacional en relación a si del contenido de la Directiva se puede desprender un derecho del particular a exigir del motor de búsqueda la eliminación de los datos que aparecen en dicho gestor debido a que estos datos e información pueden perjudicarle o que el interesado desee que estos datos e información se "olviden" tras un determinado lapso de tiempo.

En este sentido, el TJUE señala que un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. (FJ 93).

De esta manera, y ante el ejercicio del interesado de los derechos reconocidos en el Art 12.b) de la Directiva 95/46 solicitando que la inclusión en la lista

de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, de vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona, es, en la situación actual, incompatible con el Art 6.1 c) y e) debido a que esta información, habida cuenta del conjunto de las circunstancias que caracterizan el caso de autos, es inadecuada, no es pertinente, o ya no lo es, o es excesiva en relación con los fines del tratamiento en cuestión realizado por el motor de búsqueda, la información y los vínculos de dicha lista de que se trate deben eliminarse. (FJ 94).

De esta manera, ante tal solicitud, el gestor del motor de búsqueda deberá de valorar:

• Si el interesado tiene derecho a que la información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre.

• Valorar el resto de intereses legítimos en juego, concretamente, los intereses de los internautas que acceden al contenido de dicha información sobre el interesado. En estos casos será esencial entre otros aspectos a la hora de valorar este equilibrio, el papel desempeñado por el interesado en la vida pública. (FJ 99).

Decisión Final:

El TJUE considera que las actuaciones llevadas a cabo por un motor de búsqueda son consideradas tratamiento de datos, siendo en estos casos responsables de dicho tratamiento. Además, el titular de la información indexada por los buscadores puede solicitar de este último que se borre dicha información debiéndose en su caso valorarse los distintos intereses en juego que puedan estar presentes respecto de los internautas que pretendan acceder a dicho contenido.

Artículos implicados del REPD:

• Ámbito de aplicación Territorial: Art 3 Establecimiento. Considerando 22 y 23
• Definiciones: tratamiento de datos, Responsable. Art 4.
• Derecho de oposición. Art 21.
• Derecho de supresión. Art 17. Considerando 65 y 66.
• Licitud del tratamiento: Art 6.

Apartado concreto del Temario: 1.2.1, 1.2.2, 1.5.2, 1.3.2.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIAS YS Y OTROS, C-141/12 Y C-372/12, ECLI:EU:C:2014:2081

Adrián Palma Ortigosa

Abstract:

Un ciudadano le es denegado el asilo, tras ello, este último solicita a las autoridades correspondientes que se le facilite el documento dónde figuran parte de los argumentos jurídicos y datos personales de su procedimiento de denegación del asilo. (Documento conocido como minuta). La autoridad competente deniega la entrega de dicho documento, si bien, facilita otro documento donde se explicitan y resumen algunos de elementos que comprenden la minuta.

Cuestiones claves del asunto:

A) Concepto datos personales. Informe jurídico

El TJUE considera que el análisis jurídico que acompaña una resolución de denegación de asilo no es un dato personal a efectos de la Directiva, si bien, los datos personales contenidos en dicho documento, sí. (FJ 40 Y 41). Además, los datos del solicitante que figuren la minuta han de considerarse también datos personales conforme a la Directiva. (FJ 48).

B) Derecho de acceso a los datos personales

Pues bien, teniendo en cuenta que tanto el informe jurídico como la minuta contienen datos personales, el solicitante de asilo tiene derecho a conocer que datos está tratando el responsable del tratamiento sobre su persona. En este sentido, lo que se valora en este asunto es la forma en la que ha de instrumentalizarse tal derecho de acceso, es decir, como ha de facilitarse tal información o tal acceso por parte del responsable en favor del interesado.

Concretamente, la Directiva obliga a los Estados a garantizar a todos los interesados el derecho de obtener del responsable del tratamiento, libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesi-

vos, la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos. (FJ 56). La forma de garantizar y en su caso materializar esos derechos corresponde señalarla a los EEMM debiendo exigirse como mínimo que dicha comunicación sea inteligible. (FJ 57). De esta manera, cumpliéndose ese requisito formal, no es necesario que como tal se entregue una copia del documento. (FJ 58).

Decisión Final:

El TJUE señala que un solicitante de asilo puede ejercer el derecho de acceso de los datos personales que figuren tanto en la minuta en general como en el informe jurídico de dicho documento, si bien, no es necesario que dicha comunicación de esos datos sea mediante copia, sino que basta con que sea a través de un medio que garantice que esa comunicación es inteligible.

Artículos implicados del REPD:

- Derecho de acceso. Art. 15.
- Concepto de dato personal. Art. 4.

Apartado concreto del Temario: Art. 1.5 y 1.5.2**.**

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA BREYER, C-582/14, ECLI:EU:C:2016:779

Adrián Palma Ortigosa

Abstract:

El Sr. Breyer (ciudadano) consultó varias páginas web de Internet de organismos federales alemanes.

Con el objetivo de prevenir ataques y en su caso posibilitar el ejercicio de acciones penales contra piratas informáticos, estos sitios webs registran todas las consultas realizadas en dichas páginas incluyéndolas así en ficheros de protocolos. Entre los datos que se conservan en dichos ficheros se encuentran: "el nombre del sitio o fichero consultado, los términos introducidos en los campos de búsqueda, la fecha y hora de la consulta, la cantidad de datos transmitidos, la constatación del éxito de la consulta y la dirección IP del ordenador desde el que se ha realizado la consulta". El Sr. Breyer, ante tal situación, presentó un recurso con el objeto de que se prohibiera a Alemania conservar o permitir que terceros conservasen al final de las sesiones de consulta de sitios accesibles al público de medios en línea de organismos federales alemanes, la dirección IP del sistema principal delos usuarios. (FJ 13 a 17).

Cuestiones claves del asunto:

A) Concepto de Dato Personal. Dirección IP:

En primer lugar, el TJUE se centra en analizar si una dirección IP dinámica (FJ 16 y 36) puede considerarse un dato personal a los efectos de la Directiva 95/46 en relación al proveedor de servicios en línea. Para ello, el TJUE comienza señalando que una dirección IP dinámica no constituye una información relativa a una «persona física identificada», puesto que tal dirección no revela directamente la identidad de la persona física propietaria del ordenador desde el cual se realiza la consulta de un sitio de Internet. (FJ 38). Ahora bien, el hecho de que por sí sola una dirección IP dinámica no identifique directamente a una persona, si puede identificarla indirectamente. (FJ 40). Y ello es así, ya que, para calificar una información de dato personal, no es necesario que dicha información permita, por sí sola, identificar al interesado (FJ 41) o se exija en su caso

que dicha información deba de encontrarse en poder de una sola persona (FJ 43). Así, aunque la información adicional necesaria para identificar a una persona no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a internet de dicho ciudadano, hay que entender en principio, que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea pueden constituir datos personales en el sentido del artículo 2, letra a), de la Directiva 95/46. (FJ 44). Y es que, dado que hoy día el proveedor de servicios de medios en línea dispone de medios (leyes) que pueden utilizarse razonablemente para identificar, con ayuda de otras personas, a saber, la autoridad competente y el proveedor de acceso a Internet, al interesado basándose en la información de dichas IP. (FJ 48). Estas últimas han de considerarse datos a efectos de la Directiva.

B) Licitud del tratamiento:

Se analiza finalmente si el tratamiento de datos que realizan las autoridades alemanas es lícito a pesar de que no ha existido consentimiento del interesado y teniendo en cuenta que la norma solo permite el tratamiento de dichos datos con meros efectos de posibilitar y facturar el uso concreto del medio en línea por el usuario, sin que se permita a las autoridades recabar y tratar dichos datos con el objetivo de garantizar el funcionamiento general del medio en línea (FJ 54 y 55) una vez acabada la consulta de dichos servicios en línea. Pues bien, el Art 7 de la Directiva ni permite añadir nuevos principios de legitimación del tratamiento, ni tampoco permite imponer exigencias adicionales a los principios establecidos en dicho artículo (FJ 57 y 58). En el caso analizado, sin embargo, la norma ha establecido unas exigencias más restrictivas de tratamiento de datos que las reconocidas en la Directiva (FJ 59), sin que dicha normativa haya realizado una ponderación adecuada entre los intereses de los particulares y en este caso las autoridades que también ostentan dichos intereses legítimos(FJ 60) habida cuenta de las circunstancias del caso en concreto (FJ 62).

Decisión Final:

1. Una IP dinámica es un dato a los efectos de la Directiva en la medida que, si bien, por sí sola no pudiera arrojar una información que identificara a una persona, a día de hoy, existen medios que permiten poner en común varias informaciones en posesión de distintas personas convirtiéndose así en datos personales a efectos de la Directiva.

2. La norma alemana es contraria a la Directiva al no permitir que un prestador de servicios de medios en línea, en este caso autoridad pública, pueda realizar un tratamiento de datos con el objetivo de garantizar el funcionamiento general de esos mismos servicios una vez que el usuario ha dejado de consultar

dichos servicios. Hasta ese momento, la norma solo permite a dichos servicios de medios en línea conservar los datos con fines de facturación.

Artículos implicados del REPD: Art 4.1) y Art 6.1 f).

Apartado concreto del Temario: 1.2.2 y 1.3.2.

SENTENCIAS DEL TRIBUNAL SUPREMO- SALA DE LO CIVIL 672/2014 DE 19 DE NOVIEMBRE

ECLI:ES:TS:2014:5101

María Bocio Jaramillo

Abstract:

Los demandantes del presente caso interpusieron la misma contra "ADT España Servicios de Seguridad, S.L" con la que contrataron los servicios de seguridad privada a su central receptora de alarmas. Sin embargo, dicho contrato contenía una cláusula de permanencia, entendida como cláusula penal, donde si se producía la baja de los clientes en 24 meses, deberían de pagar las cantidades correspondientes a la amortización hasta la fecha de finalización del contrato.

Tras producirse la baja por parte de los demandantes sin cumplir el período de permanencia, la empresa ADT les remitió una factura con el importe a pagar y se les informó que si no se llevaba a cabo el pago serían incluidos en el registro de morosos ASNEF EQUIFAX. Al no llevarse a cabo el pago de la factura remitida, la empresa procede a la inscripción en el registro de morosos.

Los demandados interponen demanda considerando que se han vulnerado el derecho al honor y a la protección de datos del articulo 18.1 y 18.4 CE, además del artículo 29 de la LOPD y el 38 RLOPD. Pese a la interposición de esta, es desestimada en instancias previas hasta llegar ante el Tribunal Supremo.

Cuestiones claves y fundamentos de derecho:

1. Derecho fundamental vulnerado en el caso de inclusión indebida en el registro de morosos

Considera el tribunal que el derecho que se lesiona es el derecho al honor, para ello menciona la STS núm. 284/2009, de 24 de abril donde sienta como doctrina jurisprudencial que:" La inclusión indebida en un fichero de morosos vulnera el derecho al honor de la persona cuyos datos son incluidos en el fichero, por la valoración social negativa de las personas incluidas en estos registros y porque la imputación de ser "moroso" lesiona la dignidad de la persona, menoscaba su fama y atenga a su propia estimación (« pues esta clase de registros suele incluir a personas valoradas socialmente en forma negativa o al menos con recelos y reparos [...] es una imputación, la de ser moroso, que lesiona la digni-

dad de la persona y menoscaba su fama y atenta a su propia estimación »)" (FJ 4o).

2. Tratamiento de datos que se lleva a cabo en caso de solvencia patrimonial

Después de llevar a cabo una mención a los distintos instrumentos normativos que rigen la materia referente a la protección de datos, la sentencia se centra en el presente punto.

Para ello menciona el artículo 29 LOPD donde se dispone que:

"1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito solo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley ".

Hace referencia con respeto a este, que en el primer apartado se regula lo conocido como ficheros positivos o de solvencia patrimonial donde los datos son obtenidos con el consentimiento de los interesados o bien de registros públicos. Y los que se encuentran recogidos en el apartado segundo se conocen como negativos o de incumplimiento. En dichos registros los datos son facilitados por los acreedores o personas que actúen por su cuenta o interés. Por otro lado, es intranscendente que el registro haya sido consultado por terceros (FJ o4).

3. Principio de calidad de datos

Los datos deben constar con una serie de requisitos que se deducen del artículo 4 LOPD y el artículo 8 del Convenio europeo número 108 del Consejo de Europa. Por ello se exige que los datos sean: adecuados, exactos, pertinentes y proporcionales para los fines para los que fueron recogidos y tratados (FJ o4).

4. Calidad de datos en registros de morosos

En supuestos de registros de morosos, y para poder hablar de la calidad del tratamiento de los datos, menciona dos artículos determinantes en esta materia como son: el art. 29.4 LOPD que establece que "sólo se podrán registrar y ceder

los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos" y el artículo 38 RLOPD que dispone que: "para la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, se exige la existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada".

Por ello, además de que exista una deuda cierta, exigible, vencida, se exige un previo requerimiento de pago y que con dichos datos pueda valorarse la solvencia económica (FJo4).

5. Deudas de escasa cuantía

El tribunal llega a la conclusión que, si se cumplen las exigencias vistas con anterioridad, es posible la inclusión en el registro de morosos incluso de deudas de escasa cuantía. La inclusión de dichas deudas es útil para evitar, entre otras finalidades del registro de morosos, el sobreendeudamiento de los consumidores (FJ o4).

6. No cumplimiento del principio de calidad en el presente caso

Entiende el tribunal que no nos encontramos ante una deuda exigible ni cierta y que no se cumplen el resto de las prescripciones que hemos visto con anterioridad. Estamos simplemente ante una cláusula penal (FJo4).

Valoración final:

estima la demanda y considera que la inclusión en el registro de morosos es indebida, dispone que estamos ante "una reclamación derivada de la unilateral liquidación por la demandada de una cláusula penal redactada en términos que no permitían, por sí solos, fijar la cantidad en que se concretaba su aplicación. Que en la cláusula penal se previera que «en caso de que antes de concluido el plazo de permanencia 24 meses], el servicio contratado sea suspendido, dado de baja o cancelado por solicitud de baja por parte del cliente o por incumplimiento del contrato imputable al mismo, ADT ESPAÑA tendrá derecho a reclamar al CLIENTE el abono de las cantidades pendientes de amortización hasta la terminación efectiva del contrato»".

No estamos ante una deuda cierta ni exigible y no se entiende relevante dichos datos para valorar la solvencia económica de los demandados, por lo que no se cumple la proporcionalidad en la recogida y tratamiento de dichos datos. (FJo4).

Artículos del repd: Artículos 5.b y 6.b.

Apartado concreto del temario: 1.12.3. Solvencia patrimonial.

SENTENCIAS DEL TRIBUNAL SUPREMO-SALA DE LO CIVIL

SENTENCIA TRIBUNAL SUPREMO SALA CIVIL 267/2014DE 21 DE MAYO

ECLI:ES:TS:2014:2040

María Bocio Jaramillo

Abstract:

D. Gerardo, abogado en ejercicio, llevó a cabo en el año 2008 un contrato con la empresa "Yell" para obtener publicidad en las páginas amarillas acerca de su actividad profesional. Meses más tarde, hace uso de la facultad de desistimiento unilateral recogida como cláusula en el contrato para poner fin a dicha relación contractual, en este sentido, se lo comunica a la empresa a través de la dirección de correo electrónico destinada a la comunicación con clientes. En dicha comunicación, hizo constar que se le cargaran en su cuenta las respectivas cantidades referentes al tiempo en que el contrato estuvo vigente. Sin embargo, Yell hizo caso omiso de la misma, y aun recibiendo nueva comunicación del demandante, no atendió a dicha comunicación. Acto seguido, y sin previo requerimiento previo, comunicó los datos del aquí demandante al fichero de solvencia patrimonial "Asnef" del que es responsable del fichero "Equifax". "Equifax" remitió una comunicación al demandante para comunicar dicha inclusión, pero la misma fue devuelta.

El demandante, cuando tuvo conocimiento de dicha inclusión, remitió comunicación a "Equifax" para la cancelación de sus datos respectivos. A pesar de ello, denegó dicha cancelación al alegar que los datos fueron ratificados por "Yell".

El demandante procede a interponer la demanda correspondiente por intromisión de sus derechos del artículo 18.1 y 4 CE, y lo recogido en la LO 1/1982 de 5 mayo de protección de los derechos al honor, intimidad y propia imagen, además de la LO 15/1999 de protección de datos de carácter personal. Sin embargo, en instancias previas se desestimaron las pretensiones previas contra la empresa "Equifax".

Cuestiones claves y fundamentos de derecho:

1. Ámbito de aplicación de la normativa sobre protección de datos

No se excluye expresamente la actividad de comerciantes del ámbito de protección que dispone el artículo 2 LOPD. Esto no obsta para que ciertos datos de los comerciantes como: nombre comercial, domicilio... puedan ser objeto de tratamiento sin previo consentimiento ya que quedan fuera del ámbito de la ley y

del ámbito de protección del derecho a la protección de datos del artículo 18.4 CE. Si acudimos al RLOPD, aprobado por el RD 1720/2007, su artículo 2.3 excluye la actividad de navieros, comerciantes industriales y empresarios individuales, pero el tribunal considera que esta no ha sido la finalidad que persigue los instrumentos internacionales y la ley nacional a la hora de la protección de datos. Lo anteriormente estipulado lo considera extensivo a los profesionales liberales como es el caso que nos ocupa. (FJ7o).

2. Principio de calidad de datos y cancelación de datos

Los datos deben de cumplir una serie de prescripciones como son: adecuación, pertinencia, exactitud y proporcionalidad. Esto se desprende del artículo 6 del Convenio sobre protección de datos y el artículo 4 LOPD. Además, se reconoce el derecho de cancelación de los datos recogidos en el artículo 8 del Convenio europeo para la Protección de Derechos Humanos y su cancelación cuando dejen de ser necesarios o pertinentes para la finalidad para la que fueron recabados como se dispone en el artículo 4.4 y 5 LOPD. También se recoge la posibilidad de cancelar los datos cuando resulten inexactos o incompletos según el artículo 12.b de la directiva sobre protección de datos y el artículo 16 LOPD, correspondiendo a los responsables del tratamiento la comunicación de dicha supresión o rectificación como se recoge en el artículo 16.3 y 4 LOPD (FJ7o).

3. Responsable del tratamiento y del fichero en la cancelación de datos

Los ficheros de morosos regulados en el artículo 29 LOPD se conciben como una excepción al principio del consentimiento del interesado para el tratamiento de datos del artículo 6 LOPD. Sin embargo, deben cumplir con las estipulaciones referente a la calidad de los datos antes mencionadas y siguen estando vigentes las facultades reconocidas a los interesados acerca de la supresión, rectificación, entre otras.

"Equifax" es una empresa titular del fichero común en el que se incluyen los datos sobre incumplimientos de los distintos ficheros de los acreedores. Pero el hecho de ser responsable del fichero no le exime de tener que velar por la calidad de los datos o por cumplir con las facultades reconocidas a los interesados.

El art. 44.3.1o RPD prevé "que cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 LOPD , si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva, y si no recibe contestación por parte de esta entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos". Lo anterior, no puede suponer dejar las labores de rectificación, supresión, y cumplimiento de calidad de

datos en manos del acreedor, en el sentido de no rectificar o cancelar si el acreedor no lo comunica así. Si la reclamación es fundamentada y justificada, el responsable del fichero debe de llevar a cabo las facultades reconocidas al interesado.

"Equifax" no es considerada como un mero encargado del tratamiento, sino que es responsable del fichero o tratamiento y por ello debería de haber actuado ante la reclamación de supresión de datos pertinentes (FJ8o).

Valoración final:

"Equifax" tendría que haber respondido de la solicitud de cancelación de datos del demandante como responsable del fichero y, por ello, tiene que ser condenada a indemnizar al actor (FJo8 y 9)**.**

Artículos del repd: artículos 1, 5.b y 6.b, 17, 24.

Apartado concreto del temario: 1.2.1 Ámbito de aplicación, 1.5.2 Derecho de acceso, rectificación, supresión(olvido), 1.6.2 Posición jurídica de los intervinientes: responsables... etc. y 1 .12.3. Solvencia patrimonial.

SENTENCIA DEL TRIBUNAL SUPREMO-SALA DE LO SOCIAL

RESEÑA SENTENCIA DEL TRIBUNAL SUPREMO-SALA DE LO SOCIAL DE 21 DE SEPTIEMBRE 2015. ECLI:ES:TS:2015:4086

María Bocio Jaramillo

Abstract:

En el supuesto planteado nos encontramos ante un recurso de casación planteado por la empresa UNISONO frente a una serie de sindicatos, como UGT, que se personaron en instancias previas impugnando la legalidad de una cláusula contractual. Dicha cláusula dispone el siguiente contenido:" Las partes convienen expresamente que cualquier tipo de comunicación relativa a este contrato, a la relación laboral o al puesto de trabajo, podrá ser enviada al trabajador vía SMS o vía correo electrónico ... según los datos facilitados por el trabajador a efectos de contacto" y que "cualquier cambio o incidencia con respecto a los mismos, deberá ser comunicada a la empresa de forma fehaciente e inmediata». En instancias previas, se ha declarado nula la correspondiente cláusula ya que se entendió que no cumplía con el requisito del consentimiento previo en cuanto a proporcionar datos personales, contenido en el artículo 6 LOPD. Ante ello, UNISONO recurrió la correspondiente sentencia alegando que no se ha respetado el artículo 6 LOPD donde se excluye el consentimiento previo con respecto al ámbito de una relación laboral, el artículo 2.2 RLOPD donde se determina la exclusión del consentimiento en el tratamiento con referencia a datos concernientes a: teléfono, dirección postal, dirección electrónica y fax profesionales; y por último, el artículo 4 LOPD donde se recoge el uso de las datos personales de forma adecuada, pertinente y no excesiva en relación con las finalidades para las que se recabaron.

Cuestiones claves y fundamentos jurídicos:

1. Derecho fundamental

Se reconoce un derecho fundamental a la protección de datos de carácter personal en la LOPD relacionado con el artículo 18.4 CE. Además de su reconocimiento en instrumentos europeos como la Carta de Derechos Fundamentales en su artículo 8.

Se declara que estamos ante un derecho susceptible de limitaciones y que su contenido se cifra en: "incorporar un poder de disposición y control sobre los

datos personales, que constituye parte del contenido del derecho fundamental a la protección de datos, y se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Por ello, la recogida y posterior tratamiento de los datos de carácter personal se ha de fundamentar en el consentimiento de su titular, facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional, de modo que esa limitación esté justificada, sea proporcionada y, además, se establezca por Ley" (FJo2).

2. Los derechos fundamentales en la relación laboral

Se reconoce una doble limitación, en el sentido que los derechos fundamentales se encuentran limitados por los fines organizativos laborales, y que las facultades del empresario se van a encontrar limitadas por la existencia de dichos derechos (FJo2).

3. Necesidad del consentimiento en el tratamiento de datos

El TS entiende que artículo 6.2 LOPD solo excepciona del consentimiento en el ámbito laboral, aquellos datos que se consideran de "carácter necesario para el mantenimiento o cumplimiento del contrato". Por otro lado, el artículo 2.2 RLOPD excluye del consentimiento datos referentes al teléfono, email y otros, cuando sean de carácter profesional (FJ o3).

Decisión final: el TS entiende que nos encontramos ante datos de carácter no necesarios para la relación laboral y considera que dicha cláusula infringe la necesidad de consentimiento para el tratamiento de datos del artículo 6 LOPD. Concluye que nos encontramos ante un bien escaso como es el empleo y que, al determinarse la transmisión de dichos datos como cláusula contractual, teniendo presente la posición más débil del trabajador en la relación laboral, no puede hablarse de un verdadero consentimiento del artículo 6 LOPD (FJ. 3o).

Artículos del redp: Artículo 7,88 y Considerandos 42 y 155.

Apartado concreto del temario: 1.4.1 Consentimiento: otorgamiento y revocación.

SENTENCIAS DEL TRIBUNAL SUPREMO-SALA DE LO CIVIL

RESEÑA SENTENCIA TRIBUNAL SUPREMO SALA CIVIL 12/2014 DE 22 DE ENERO

ECLI:ES:TS:2014:355

María Bocio Jaramillo

Abstract:

Los demandantes José Enrique y Elisenda interponen recurso de casación contra la sentencia dictada en el ámbito de apelación por la cual se desestima su pretensión referida a los siguientes argumentos. Nos encontramos con la Sociedad Cash Canarias S.L que solicitó préstamo a Caja Rural Canarias apareciendo como avalistas los aquí demandantes junto con otros sujetos. Con respecto a la deuda surgida del préstamo, se produce una causa anticipada de resolución del préstamo, con lo que la misma se hace exigible a la empresa y sujetos mencionados, procediendo la entidad bancaria a la resolución del mismo y transmitiendo los datos personales de los obligados a sendos registros de morosos. Se lleva a cabo por la entidad bancaria el procedimiento de ejecución dineraria sin habérsele notificado a los mismos y, en ese ínterin, se produce el pago de una serie de cantidades por parte de los aquí demandantes. Sin embargo, dichas cantidades no se vieron reflejadas como disminución del total a deber que aparecía en el registro de morosos. Habiendo procedido los mismos al intento de modificación de sus datos, dichos intentos fueron infructuosos, procediéndose incluso por parte de doña Elisenda, a la reclamación ante la AEPD.

Se considera por parte de los demandados que nos encontramos ante la vulneración de su derecho al honor, intimidad personal y propia imagen del artículo 9.2 LO 1/1982 de 5 de mayo y los artículos 4.1,4.3 y 29 LOPD 15/1999 y artículo 38 RLOPD aprobado por RD 1720/2007 RPD.

Cuestiones claves y fundamentos jurídicos:

1. Derecho a la protección de datos y sus dos esferas

Hace mención a la regulación existente a nivel internacional e interna acerca del derecho a la protección de datos y considera que se diferencia un facultad positiva y negativa de este. Así menciona al TC para afirmar: "un contenido negativo (limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos), este

derecho fundamental tiene un contenido positivo, la atribución al afectado de determinadas posibilidades de actuación, de ciertas acciones para exigir a terceros un determinado comportamiento".

Por otro lado, estipula que la recogida y tratamiento de datos deben de ir presididas por el principio de calidad de estos, entendido como la adecuación, pertinencia, proporcionalidad y exactitud de los datos. Esto se deriva de lo dispuesto en el artículo 6 de la Directiva 1995/46 CE relativa a la protección de datos y el artículo 4 LOPD (FJo3).

2. Los registros de morosos

Aludiendo a su existencia en el artículo 29 LOPD, menciona su finalidad de probar la solvencia económica de las personas inscritas en ellos. Como excepción al previo consentimiento necesario para el tratamiento de datos, hace referencia a la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por un tercero al que se le comunique dicha información, siempre y cuando, venga recogido por una Ley. A esta excepción hace referencia el artículo 29. 2 cuando menciona los datos personales relativos al incumplimiento de obligaciones dinerarias facilitados por el acreedor sin el consentimiento del afectado" (FJo4).

3. Incumplimiento del requisito de calidad de datos comunicados al registro de morosos

Entiende que no se ha cumplido las exigencias de calidad, entre ellas, menciona la exactitud de la deuda ya que no se corresponde la cantidad que aparece en el registro de morosos con lo debido. Tampoco se podía considerar como una deuda vencida y exigible, artículo 38 LOPD, ya que se trataba de una estimación hecha por la entidad bancaria que no se correspondía con los hechos. (FJo5).

Valoración final: se considera infringido el derecho a la protección de datos por no haberse cumplido los requisitos de calidad. Concretamente el tribunal haciendo referencia a la doctrina de su sala considera que:" «La inclusión en los registros de morosos no puede ser utilizada por las grandes empresas para buscar obtener el cobro de las cantidades que estiman pertinentes, amparándose en el temor al descrédito personal y menoscabo de su prestigio profesional y a la denegación del acceso al sistema crediticio que supone aparecer en un fichero de morosos [...] Por tanto, esta Sala estima que acudir a este método de presión representa en el caso que nos ocupa una intromisión ilegítima en el derecho al honor de la recurrente, por el desvalor social que actualmente comporta.

Estar incluida en un registro de morosos y aparecer ante la multitud de aso-

ciados de estos registros como morosa sin serlo, que hace desmerecer el honor al afectar directamente a la capacidad económica y al prestigio personal de cualquier ciudadano entendiendo que tal actuación es abusiva y desproporcionada, apreciándose en consecuencia la infracción denunciada.» (FJo5).

Artículos del repd: Artículos 5.b y 6.b.

Apartado concreto del temario: 1.12.3. Solvencia patrimonial.

SENTENCIAS DEL TRIBUNAL SUPREMO-SALA DE LO CIVIL

RESEÑA SENTENCIA TRIBUNAL SUPREMO SALA CIVIL 12/2014 DE 22 DE ENERO

SENTENCIAS DEL TRIBUNAL SUPREMO. (SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO)

STS 5178/2014 - ECLI: ES:TS: 2014:5178

Adrián Palma Ortigosa

Abstract:

Empresa solicita a la AEPD iniciar procedimiento sancionador contra CaixaBank por la inclusión de esta sociedad en el fichero de la Central de Información de Riesgos del Banco de España al haber realizado una asociación indebida de los datos de dicha empresa a una deuda reclamada. La AEPD acordó no incoar actuaciones inspectoras ni iniciar procedimiento sancionador al ser la parte denunciante una sociedad mercantil, considerando que dicho asunto excede del ámbito competencial de la reseñada Agencia.

Cuestiones claves del asunto:

A) Ámbito de aplicación subjetivo:

En esta sentencia se valora si la normativa en materia de protección de datos es aplicable a las personas jurídicas, es decir, lo que se viene a debatir es si las personas jurídicas son titulares o no del derecho a la protección de datos. En este sentido, el TS llega a la conclusión de que las personas jurídicas no son titulares de tal derecho por las siguientes razones.

En primer lugar, el TS señala que del conjunto de normativas tanto españolas como europeas que configuran y perfilan el derecho a la protección de datos, ninguna de ellas hace mención a las personas jurídicas, sino que en todo momento su protección se circunscribe a la protección de las personas físicas. (FJ 5o).

En segundo lugar, respecto a una hipotética vulneración del principio de igualdad, el TS señala que tampoco ha de estimarse el motivo, ya que, ante la desigualdad que ofrece la distinta realidad de las personas jurídicas frente a las personas físicas o humanas, la consecuencia de diferenciar su tratamiento nor-

mativo en determinados ámbitos del Derecho (como ocurre en la protección de datos personales) resulta coherente. Además, y en alusión a lo que indica el Fiscal, el hecho de que no exista un norma que proteja a las personas jurídicas en materia de protección de datos no deja a estas últimas en una completa desprotección por parte del ordenamiento, ya que, por ejemplo, la inclusión indebida en un registro de insolvencia puede constituir intromisión ilegítima en el derecho al honor al tratarse de una imputación que lesiona la dignidad de la persona, menoscaba su fama y atenta a la propia estimación, teniendo reconocido las personas jurídicas jurisprudencialmente la protección del derecho al honor, a la intimidad personal y a la propia imagen que garantiza el artículo 18.1 CE (STC 214/91 y 139/95), reconocimiento que sin embargo no habilita para permitir que su extensión alcance también a la protección de datos. (FJ 6o).

Decisión Final: Las personas jurídicas no son titulares del derecho a la protección de datos. De manera que una empresa no puede acudir a la AEPD para exigir que se le aplique la normativa en materia de protección de datos .

Artículos implicados del REPD: Art 1. Y Considerando 14.

Apartado concreto del Temario: 1.2.1. Ámbito de aplicación subjetivo.

SECTION III: USE CASES

Challenge Title: Data in the Healthcare sector	
Use Case Author	*Adrián Palma Ortigosa and Sara Lorenzo Cabrera, Universidad Sevilla*
Topic	*Privacy in Health*
Overview	*The Hospital "Virgen del Rocío" of Sevilla is made up of a staff of more than 300 healthcare professionals and has a unit specialized in the study and treatment of patients suffering from severe headaches, migraines and sleep-related problems.* *In the last year, this unit has received European funding to carry out researchs that seeks to link certain eating habits to certain types of headaches. The management team has decided to collect a number of personal data to start the investigation. In particular, the following documents shall be used:* *– Medical records of those patients who have been treated in the hospital for research-related illnesses.* *– Up to a total of 10,000 clinical records of patients with the same symptoms of the rest of the hospitals of the public health service in Andalucía.* *– Up to a total of 5000 medical records from other hospitals in the European Network to which the hospital belongs.* *Clinical tests of patients (hospital users or not) suffering from any of the diseases described above. The clinical trials will bring together a segment of the population ranging from 14 to 50 years old.*
1. Engage	
Big idea	*Medical research in the health sector.*

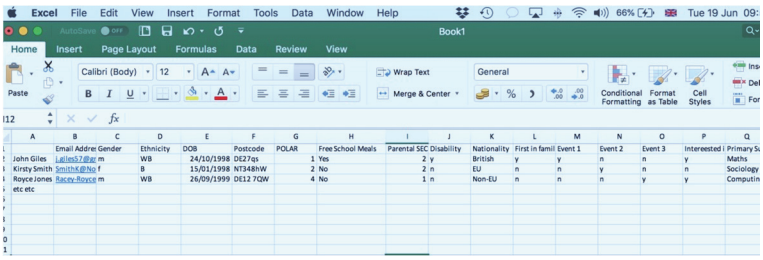
Essential Question	*Is the research that the hospital carries out viable from the point of view of data protection?*
Initial resources	*Students will be given a document specifying the complete research project and the personal data to be collected.* *In addition, the students will be able to watch two videos on health research and data protection that are proposed as initial resources:* *– https://renovatiobiomedica.com/2018/02/08/nrd- proteccion-datos-ue-bigdata-sanitario-evaluacion-impacto- una-herramienta-proteccion-la-privacidad/.* *– http://www.comda.tv/video-296_novedades-del- reglamento-general-de-proteccion-de-datos-en-la-asistencia-e-investigacion-sanitaria-·-1-de-marzo-de-2018.html-*
Guiding Questions	*Students must act as if they were the DPO of the hospital. Before going deeper into the subject, they have to analyse what personal data are they going to collect and process, for what purpose, what will be the legal basis, who will be the unit responsible for the processing, etc.* --- *To this end, students will carry out a briefing room exercise, in which they will decide what questions or information to ask the unit responsible for the research to begin framing the task.* *The brain storming exercise will be completed with the elaboration of a mental map, which will be of great help for the students (for example, they can use the following tool: https://coggle.it/).* *Questions asked by students:* (…)
Reflections	*According to the list of questions:* *– Would you classify the questions in priority order or according to any other criteria?* *(We think that a different classification can raise new information and knowledge)* *– Would you change the priority order of the questions?* *– Would you remove any question from the list because you think it is not necessary?* *– Would you introduce into the list any question that you feel is missing?*

	– Do you think that this exercise is useful as a starting point? *– Can you think of another way to initially address the problem?* *– Do you believe that the given list of questions takes into account the complexity of the legal problem?* *– (...)* *Individual reflections on the process* *– (...)*
Other notes	*Suggestions for dealing with the brainstorming exercise:* *1. The teacher is the driver of the brainstorming exercise.* *2. The teacher has to create an understanding atmosphere in which the students can express their ideas freely and confidently.* *3. The teacher and students have to respect others ideas, because all ideas, although it can be initially seen as nonsense, have value to address the suggested problem.*
2. Investigate	
Activity Description	*Encourage students to map out a process of investigation for answering the questions above.*
Resources	*• Working Document on the processing of personal data relating to health in electronic health records (EHR). Adopted on 15 February 2007. Article 29 Data Protection Working Party. Available in: https://www.apda.ad/system/files/wp131_es.pdf* *• Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research. Available in: https://www.hhs.gov/sites/default/files/hipaa-future- research-authorization-guidance-06122018%20v2.pdf* *• Web site. ICO. Information Commissioner´s Office https://ico.org.uk/for-organisations/resources-and-support/health-sector-resources/*
Synthesis	*In order to understand the main data protection implications of this project, the research management team asks you to write a short report. (2-3 pages). ---* *The students should not explain the concrete measures, but only refer to them, relating them to the project proposed by the management team.*

Reflections	*Please provide a reflection on the process:* *1. What are the key problems to overcome in this challenge?* *2. How did you organise the work involved in the investigation?* *3. How did you collect additional data? What worked well about this? What information gaps were still present at the end?* *4. How successful was the investigation process?*
Other notes	*None.*
3. Act	
Solution Proto-types	*Prepare a full legal report analyzing all the legal consequences you consider appropriate related to the implementation of the research project to which the research team refers. Please, take into account any implication that may affect the right to data protection of patients.*
Solution	*Please, indicate your key recommendations to the Direction Team here:* *(…)*
Implementation plan	*Please, develop a plan for the implementation of the legal report.*
Evaluate	*Please develop a journal entry which answers the following questions:* *1. What measure(s) do you consider necessary to implement since the design stage?* *2. What measures do you think will generate the most rejection from the management team?* *3. What were the strengths and weaknesses of your overall legal report?*
Other notes	*None.*
4. Reflection and documentation	

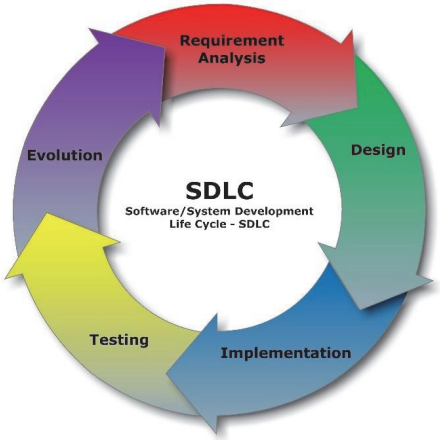
Case notes	*Students must assess the legal suitability of this project in relation to data protection. Among the items that must be taken into account:* *– Legal bases that allow the processing of data.* *– Regarding consent: That consent must be informed, need to inform about the possibility of withdrawing such consent, consent without a clearly defined purpose.* *– Processing of minors' personal data.* *– Data conservation period.* *– Implementation of security measures (encryption, pseudonymization)* *– Possibility of anonymizing personal data.* *– Personal Impact Assessment.* *– Contingency plan for possible security breaches or incidents.*

Challenge Title: Data Security and University Widening Participation Services	
Use Case Author	*Alex Nunn, University of Derby*
Topic	*Privacy in Public Administration*
Overview	*You are working as an assistant DPO in a large Post-92 University. Universities in the UK are encouraged to widen participation in Higher Education from groups that are traditionally less represented in HE. As such, the Widening Participation team have been working with local schools and undertaking events with children, including those from groups that are less represented in HE. Where these are sixth form students they are often invited into the University and WP team keep a register of these young people so that they can track the effectiveness of their outreach activities by surveying the young people to see how many were applying to University and the different Universities they applied to. Your task is to advise on what data that is currently stored should be kept and used and what arrangements can be made into the future to ensure the effectiveness of these activities.*
1. Engage	
Big idea	*Widening Participation Mapping Data Storage and Future Requirements*
Essential Question	*How can the Widening Participation team best learn about the effectiveness of outreach services while maintaining the privacy of data?*
Initial resources	*Outreach activities undertaken by Universities: https://www.officeforstudents.org.uk/advice-and-guidance/promoting-equal- opportunities/national-collaborative-outreach-programme-ncop/* *Data on WP in HE: https://www.gov.uk/government/statistics/widening-participation-in-higher-education-2017*
Guiding Questions	*You receive a call from the head of the Outreach team who did the internal online training on GDPR and is worried that his team are not compliant. He asks for advice on whether the data the team already holds from prvious outreach activity is GDPR compliant and how she can go about providing WP services, ensuring that they are effective and being GDPR compliant.* *---*

	What questions should you ask of the WP Manager to start to frame the task? Brainstorm a list of questions you should ask when you call the WP Manager back.
Reflections	*1. Complete your learning journal and answer the following questions:* *2. What is interesting about this challenge?* *3. How did you feel about the initial brainstorming exercise?* *4. Were you happy with the list of questions you put together? Why/why not?*
Other notes	*None.*
2. Investigate	
Activity Description	
Resources	*Some resources to get you going:* *When you ring the WP manager back they explain that they have collated data on users of their services from a variety of sources. Schools provided data on pupils names, post-code and basic characteristics (DoB, post-code) and other data was collected from the individuals in a survey of their interests, confidence and about their background. Some of this information is necessary so that the manager can ensure that funding received from the National Collaborative Outreach Programme is being used in accordance with funder requirements and some of the data collected results from the team's research informed ideas about the types of factor that might affect aspirations to study at University.* *The data held at present looks like this:*  *The Manager informs you that it has been previous practice to re-survey the contacts in order to find out what they actually did and what affect the outreach activities had on their decisions. In the past the team say that they have collected permissions to undertake this second*

	survey when they undertake the first round of data collection. This is via box that the students can untick if they do not want to receive the second survey. The data was initially collected via an IPad and survey app – but this is the only data that remains. *https://www.youtube.com/watch?v=RZUlsdyREvg&feature=youtu.be* *---* *Please provide a list of additional resources that you have found and are useful in the task.* *Do you need to collect any other form of data* *How will you collect this? Develop and implement a plan for collecting this information. Ensure that you meet your own Data Protection and ethical requirements.*
Synthesis	*Please roll-play a telephone conversation within the group to document the advice you would give the manager. Students watching should appraise the advice offered.*
Reflections	*Please provide a reflective statement in your journal to summarise your answers to the questions below:* *1. What are the key problems to be overcome in this challenge?* *2. How did you organise the work involved in the investigation?* *3. How did you collect additional data? What worked well about this? What information gaps were still present at the end?* *4. How successful was the investigation process? How would you organise the work differently if you did it again?*
Other notes	*None.*
3. Act	
Solution Prototypes	*As individuals please draft a clear email and any further documentary advice that you wish to send to the manager as a follow up to the telephone conversation.*
Solution	*Please provide a copy of that email here.*
Implementation plan	*Please draft an action plan that you would expect the WP team to complete to show that they have made their activities GDPR compliant.*
Evaluate	*Please develop a journal entry which answers the following questions:* *1. What are the key challenges for WP teams in Universities in implementing the plan you identified?*

	2. What were the strengths and weaknesses of your overall approach to the challenge? *3. Were there any changes that could be made to the investigation process, phone conversation, the email and implementation plan plan to make them more effective, based on your reflection on the whole challenge?* *4. If you were to run this challenge with a group of learners, how would you change it?* *5. What else did you learn from this process?*
Other notes	
4. Reflection and documentation	
Case notes	

Challenge Title: Enhancing Children's Privacy Awareness	
Use Case Author	*Roberto Montanari, Elisa Landini, Aura Tardia, RE:Lab*
Topic	*Privacy in Minors*
Overview	*The Italian SME Game&Learn s.r.l. develops apps and software addressed at children and teenagers.* *Their products allow children to play games while also learning new things. In order to design the software effectively, the company usually carries out tests with users to validate or improve the product throughout the software development cycle.*
1. Engage	
Big idea	*Children and technology development.*
Essential Question	*How to ensure that children are fully aware of the data they provide.*
Initial resources	*The Software Development Life Cycle entails a phase of testing with real users. The testing phase is extremely important for designers to understand the reactions of users to the software, evaluate its usability, and to devise any fixes or improvements based on test results*  *An introduction reading to user testing with children: https://www.nngroup.com/articles/childrens-websites-usability-issues/*

Guiding Questions	*You are Game&Learn's newly appointed DPO. While collecting information from the company's management and employees to define the processes you will follow and the potential risks and vulnerabilities, you also speak with the User Testing team.* *They explain that they believe to have always been very conscious about the privacy of the children/teenagers and have always asked for the written consent of the parents before performing the tests.* *They are unsure whether they now need to also provide information on the type and purposes of the data processing directly to the children, and in that case, they would like to draft a general document to use to that end, to be adapted to specific cases.* --- *Use this space to show how you will do this. And Leave space for the students to complete the questions. This box should be completed as a team by the students* *What questions should you ask the User Testing team to start to frame the task?* *Brainstorm a list of questions you should ask in order to get a clearer picture of the activity and of the role you could play.* *Draft a complete list of questions and put them in an order, prioritizing the ones you believe are more important.*
Reflections	*1. Once the students have done this. Encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge?* *2. How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process.* *3. Reflect on the Guiding Questions process and results:* *4. How did you feel about the initial brainstorming exercise?* *5. Were you happy with the list of questions you put together? Why/why not?*
Other notes	
2. Investigate	
Activity Description	*Now that you have identified the information you need from User Testing team, collect the resources that can help you develop a good solution.* *The Investigation phase should lead you to the answers to your Guiding* *Questions.*
Resources	*Some resources to get you going:*

	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection- regulation-gdpr/applications/children/ https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 *----* *Encourage students to collect and use resources to help them to address the question.* *Try and gather more resources that might help you address the challenge more effectively.*
Synthesis	*Develop a short document (2 pages max.) containing Guidelines for the drafting of child-friendly privacy information. This should also contain an introductory part where you can try to explain the process you followed to develop the Guidelines to your colleagues in the User Testing team.* *---* *Encourage students to summarise their answer.*
Reflections	*1. Students to provide a reflection on the process. Reflect on the Investigation phase:* *2. What are the key problems to be overcome in this challenge?* *3. How did you organize the work for the development of the Guidelines?* *4. How did you collect additional information and resources?* *5. How successful was the investigation process? How would you organize the work differently if you did it again?*
Other notes	
3. Act	
Solution Prototypes	*Design an "Information on the Processing of Personal Data" document that can be used to effectively communicate with children in compliance with the principle of transparency.* *You can experiment different formats for this Privacy Notice, which may include images, icons or other elements that might facilitate their understanding.*
Solution	*Students to provide a solution or options for different solutions in the format suggested above.* *Please insert the final version of the Information on the Processing of Personal Data here:*
Implementation plan	*Students also to provide a plan for how at least one of the solutions should be delivered.*

	Develop a procedure to help the Game&Learn employees to use the document you've created in the right way (e.g. in terms of timing, modalities, and so on)
Evaluate	*Students to develop a journal entry to evaluate the different solutions, and how they might go about the exercise differently in future. Students might also be asked how the exercise itself could be further developed as a pedagogical process.* *Develop a journal entry evaluating the solution you identified:* *1. What are the key challenges that the User Testing team may encounter in following the procedures?* *2. What were the strengths and weaknesses of your overall approach?* *3. What changes would you make to your Guidelines and to your Privacy Notice?* *4. What did you learn from this process?*
Other notes	
4. Reflection and documentation	
Case notes	

Challenge Title: Processing activity records	
Use Case Author	*Davide Borelli, Lucilla Gatt, Suor Orsola Benincasa University of Naples*
Topic	*Privacy in Banking*
Overview	*'UOMe' is an Italian fintech company headquartered in Milan and regulated by the Italian Conduct Authority. Being particularly active in the Forex market, 'UOMe' offers low-priced currency exchange and international payments to private individuals and companies.* *Although many of its activities are deeply based on technology (e.g., lead qualification, KPI), 'UOMe's business model heavily relies on traditional 'call calling': having identified a 'prospect', a salesperson calls them to pitch 'UOMe's products and services. Once onboarded, clients may use 'UOMe's mobile app to get real-time quotes, place trades, make transfers, and manage their existing positions.* *'UOMe' Operations Team is based in India, whereas the Sales and the Compliance Offices are respectively based in Italy and the United Kingdom.* *Being successfully pitched by one of 'UOMe's dealers, Davide decides to join the service conscious of the convenience of the offered rates. Nevertheless, while going through the onboarding process he suddenly realises that the service is not cheap as expected in the first place, hence he decides not to progress with his application. After a couple of weeks, having received another unsolicited call from 'UOMe', Davide decides to exercise his rights to access and to be forgotten.*
1. Engage	
Big idea	*Processing Activity Records and Data Subject Rights (DSRs)*
Essential Question	*How would you define for each processing activity which is the appropriate legal basis for processing? How would you ensure you have full control and visibility over your data processing activities? How would you comply with a data subject request (e.g., right to access, to deletion, etc.)?*
Initial resources	*1. A brief Onboarding Standard Operating Procedure* *2. The request sent by the data subject* *3. A Processing Activity Inventory spreadsheet*
Guiding	*Acting as newly appointed Global Privacy Offices, the Students*

Questions	*should try to update the existing Onboarding Standard Operating Procedure to include necessary privacy controls, document the related processing activity into an ad hoc inventory spreadsheet, and handle the data subject request.* • *What controls would you put in place to ensure that privacy is considered throughout the onboarding process?* • *In the financial sector, is there any regulations that might have an impact on the applicability of the data protection legislation?* • *How would you limit unstructured data transfers?* • *How would you capture the data given by prospects and clients in compliance with the applicable data protection legislation?* • *How would you handle data subject requests? Would you structure a proper process or handle them manually on a case by case basis? What if the request has been sent using a third-party platform (e.g., One.Thing.Less)?*
Reflections	*Once the exercise is completed, the Students will be encouraged to reflect on the challenges that the financial sector players may face from a privacy perspective and on the importance of a data mapping exercise. The Students will also be encouraged to think about how a similar scenario could be tackled more effectively in future and to record any individual reflections on the exercise.*
Other notes	*None.*
2. Investigate	
Activity Description	*Each Student is required to map out a process of investigation for answering the questions above.*
Resources	• *Tackling nuisance calls and messages: Consultation on action against rogue directors (30 May 2018), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attac_hment_data/file/711999/Nuisance_calls_and_texts_consultation 1_.pdf* • *Lawfulbasis for processing (2018), available at https://ico.org.uk/for- organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis- for-processing/* • *Draft List of types of Data Processing Operations which require a Data Protection Impact Assessment (6 June 2018), available at https://www.dataprotection.ie/docimages/documents/DPIA%20for%20consultation.pdf* • *Information to be Given (March 2018), available at https://www.dataci.gg/wp- content/uploads/2018/03/InfoGiven.pdf* • *Conditions for Processing (March 2018), available at https://www.dataci.gg/wp- content/uploads/2018/03/Conditions.pdf*

	• *Information Commissioner: A Closer Look at Rights & Remedies, available at_https://www.inforights.im/media/1441/rights_and_remedies.pdf* • *Report on Innovative Uses of Consumer Data by Financial Institutions (28 June 2017), available at http://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+use s+of+data+2017.pdf* • *Guidelines on transparency under Regulation 2016/679 | WP260 rev.01 (11 April 2018), available at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51 025* • *Data Protection Guidelines for Banks (8 May 2018), available at https://idpc.org.mt/en/Press/Documents/Data%20Protection%20guidelines%20for%20banking.pdf*
Synthesis	*In groups of 5, the Students are required to create a PowerPoint presentation which outlines –* *(1) Their findings on the topic,* *(2) How they would update the existing Onboarding Standard Operating Procedure,* *(3) How they would record processing activities within a proper inventory, and* *(4) Their strategy to handle the data subject request.* *The proposal shall be shown to and discussed with the class. Afterwards, the groups shall engage the data subject to handle its request. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach*
Reflections	*The Students will be encouraged to reflect on the operational side of privacy and on how to foster awareness and accountability within the business. They will also be encouraged to think about how a similar scenario could be tackled more effectively in the future and record any individual reflections on the exercise.*
Other notes	*None.*
3. Act	
Solution Prototypes	*Each Group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this.* *The above-mentioned briefing shall include the following –* *1. An explanation of the Know Your Customer (KYC) process and any suggested updates,* *2. What risks may be associated with the onboarding of new clients,* *3. An introduction to the different legal basis for processing,* *4. A data mapping inventory handling workflow,*

	5. A data subject rights handling procedure, and *6. A brief strategy to handle the request made by Davide.* *The recommendations provided should aim to improve attitudes to data privacy and security, as well as awareness of the implications of breaches of the privacy laws and regulations.* *The proposal shall be shown to and discussed with the class. Each group shall evaluate* *the performance of the others and outline pros and cons of each suggested approach.*
Solution	*The Students shall provide a solution or options for different solutions in the format suggested above.*
Implementation plan	*The Students shall provide a plan on how the solutions may be delivered, and how to foster a virtuous change management within the business.*
Evaluate	*The Students shall answer the following –* *1. What are the strengths and weaknesses of the approach you have suggested?* *2. How did you assessed the proposed trade-off between legal compliance and business needs?* *3. What did you learn from this exercise?* *The Students will also be required to carry out a SWOT analysis on one of the suggested approaches.*
Other notes	*None.*
4. Reflection and documentation	
Case notes	*It can be developed in future by showing real onboarding procedures and let them assist a real contract negotiation.*

Challenge Title: Vendor Risk Management and Data Protection Agreement negotiation	
Use Case Author	*Davide Borelli, Lucilla Gatt, Suor Orsola Benincasa University of Naples*
Topic	*Data Protection Law*
Overview	*'Ego' is an Italian cosmetic company headquartered in Milan. It focuses on hair colour, skin care, sun protection, make-up, perfume, and hair care. Its Head of Marketing, Jane, is currently working on a new web campaign to advertise Ego's brand new green tea mask: her plan is to create a website where people can purchase the new product or simply subscribe a newsletter to receive exclusive offers and the latest news on Ego's products.* *To run this campaign, Jane decides to use a Software as a Service (SaaS) solution named 'Bazaar', i.e., a US e-commerce platform for online stores and retail point-of- sale systems. As such, she contacts all the relevant internal stakeholders (i.e., Procurement, InfoSec, and Privacy) to get the new Vendor on boarded sooner.*
1. Engage	
Big idea	*Vendor Risk Management and Data Protection Agreement Negotiation.*
Essential Question	*How would you ensure that the use of third-party products, IT suppliers and service providers does not result in a potential business disruption or in any negative impact on business performance? How would you ensure that any third-party complies with the applicable data protection legislation? How would you make sure that a cross-border data transfer does not result in a material circumvention of the applicable privacy legislation?*
Initial resources	*1. A description of the web marketing campaign* *2. A brief Vendor Onboarding Process* *3. A Data Processing Agreement (DPA) Template* *4. Standard Contractual Clauses (SCC) Template*
Guiding Questions	*Acting as newly appointed Global Privacy Offices, the Students should try to update the existing Vendor Onboarding Process to include appropriate privacy controls and negotiate an ad hoc DPA and (where needed) SCCs.* • *What control would you put in place to ensure that every Vendor complies with the applicable data protection legislation?* • *Is there any sort of due diligence which might be carried out to*

	assess potential privacy risks? If so, what should be the content of such a due diligence? • *How would you negotiate a DPA? What are the main challenges? What would you focus on?* • *What if the processing activity results in a cross-border data transfer? What safeguards are you required to put in place to ensure that such a transfer does not result in a circumvention of the applicable legislation?*
Reflections	*Once the exercise is completed, the Students will be encouraged to reflect on the challenges of the vendor risk management from a privacy perspective. The Students will also be encouraged to think about how a similar scenario could be tackled more effectively in future and to record any individual reflections on the exercise.*
Other notes	*None.*
2. Investigate	
Activity Description	*Each Student is required to map out a process of investigation for answering the questions above.*
Resources	***Vendor Risk Management*** • *Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR (14 May 2018), available at http://gdprandyou.ie/wp- content/uploads/2018/05/Guidance-for-Data-Processing-Contracts-GDPR.pdf* • *What should be contained in a contract between a Data Controller and a Data Processor?, available a https://www.dataprotection.ie/docs/710-What- should-be-contained-in-a-contract-between-a-Data-Controller-and-a-Data- Processor/654.htm* • *ICO GDPR guidance: Contracts and liabilities between controllers and processors (13 September 2017), available at https://ico.org.uk/media/about- the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for- consultation-september-2017.pdf* • *Technical Note: Benefits of a new data protection agreement (7 June 2018), available at https://assets.publishing.service.gov.uk/government /uploads/system/upload s/attachment_data/file/714677/Data_Protect ion_Technical_Note.pdf* ***Cross-border Data Transfers*** • *The eighth data protection principle and international data transfers, available at https://ico.org.uk/media/for- organisations/documents/15 66/international_transfers_legal_guidance.pdf* • *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (30 May 2018), available at https://edpb.europa.eu/sites/edp*

	b/files/files/file1/edpb_guidelines_2_2018_ derogations_en.pdf • *Draft Guidelines on Article 49 of Regulation 2016/679 | WP 261 (12 February 2018), available at http://ec.europa.eu/newsroom/article 29/document.cfm?doc_id=49771* • *Adequacy Referential | WP 254 rev.01 (9 February 2018), available at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49724* • *Data transfers abroad for outsourced data processing, available at https://www.edoeb.admin.ch/dokumentation/00153/00184/00189/index.ht ml?lang=en*
Synthesis	*In groups of 5, the Students are required to create a PowerPoint presentation which outlines* *(1) Their findings on the topic,* *(2) How they would update the existing Vendor Onboarding Process, and* *(3) Their contractual strategy with 'Bazaar'.* *The proposal shall be shown to and discussed with the class. Afterwards, the groups shall engage 'Bazaar's Legal Counsel, Davide, to negotiate any necessary agreement on data protection. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.*
Reflections	*The Students will be encouraged to reflect on the operational side of privacy and on how to foster awareness and accountability within the business. They will also be encouraged to think about how a similar scenario could be tackled more effectively* *in the future and record any individual reflections on the exercise.*
Other notes	*None.*
3. Act	
Solution Prototypes	*Each Group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this.* *The above-mentioned briefing shall include the following –* *1. An explanation of the Controller-Processor relationship* *2. What risk may be associate with the onboarding of new suppliers* *3. A brief explanation of how to conduct an audit/due diligence on a given supplier (and its products and services)* *4. An updated Vendor Onboarding Process* *5. A strategy for cross-border data transfers*

	6. A brief strategy to negotiate the contract with the supplier *7. Pros and cons of the suggested approach* *The recommendations provided should aim to improve attitudes to data privacy and security, as well as awareness of the implications of breaches of the privacy laws and regulations.* *The proposal shall be shown to and discussed with the class. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.*
Solution	*The Students shall provide a solution or options for different solutions in the format suggested above.*
Implementation plan	*The Students shall provide a plan on how the solutions may be delivered, and how to foster a virtuous change management within the business.*
Evaluate	*The Students shall answer the following –* *1. What are the strengths and weaknesses of the approach you have suggested?* *2. How did you assessed the proposed trade-off between legal compliance and business needs?* *3. What did you learn from this exercise?* *The Students will also be required to carry out a SWOT analysis on one of the suggested approaches.*
Other notes	*None.*
4. Reflection and documentation	
Case notes	*It can be developed in future by showing real onboarding procedures and let them assist a real contract negotiation.*

Challenge Title: Video Surveillance in the Workplace	
Use Case Author	*Adrián Palma Ortigosa, Universidad of Sevilla*
Topic	*Data Protection Law*
Overview	*Zapatiesta, S. L., is a Spanish company that designs and manufactures toys for children between the ages of 2 and 12.* *This company has a total staff of 155 employees, each employee is distributed in different areas according to their job functions. This company also has a nursery service where workers can leave their children while they do their work.* *In recent months, the company's management has been informed that some workers have robbed the company, so the production has decreased in the area dedicated to the manufacture of toys for babies.* *On the other hand, Zapatiesta, S. L., aims to develop new and better products that could have a great acceptance in the market. Before supplying the toys on the market, the company will analyze the behavior and reaction of the children, making this experiment with children of the workers who attend the nursery.* *In conclusion, the company have decided to install a video surveillance to check the performance of employees, analyze the market conduct in the company nursery and prevent the thefts.*
1. Engage	
Big idea	*Video surveillance in the workplace.*
Essential Question	*Does the implementation of a video camera system in the facilities of the company Zapatiesta, S. L., fit the purpose?*
Initial resources	*a) Report from the Marketing Department proposing the management of the company a real-time recording of the children's reactions to the delivery of toys in the testing phase designed by Zapatiesta, S. L.* *b) Report from the Quality and Control Department warning the company's management of the continuous loss of a large quantity of materials, both during working and non-working hours.* *Report from the Human Resources Department warning the company's management of a decrease in production in a specific area of the organization.*

Guiding Questions	*As the Data Protection Officer of Zapatiesta, S. L., the CEO would like to know if there is any kind of problem or objection regarding the installation of the cameras in the areas previously indicated.* *---* *What kind of questions should you ask yourself as this company DPO? What questions would you ask the CEO or any of the Departments to complete the necessary information to help you come to a decision?*
Reflections	*Complete your learning diary and answer the following questions:* *1. What is the most interesting part of this challenge?* *2. Were you satisfied with the list of questions that were proposed?*
Other notes	*Any other notes that teachers and students should be aware of when using this challenge.*
2. Investigate	
Activity Description	*Encourage students to map out a process of investigation for answering the questions above.*
Resources	*Some resources to get you going:* *Documents:* *• Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. ARTICLE 29 Data Protection Working Party* *Available:http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf* *• Instruction 1/2006, of 8 November, of the Spanish Data Protection Authority, on the processing of personal data for surveillance purposes through camera or video camera systems.* *More information in: https://www.aepd.es/areas/videovigilancia/index.html*

	 --- *Please provide a list of additional resources that you have found and are useful in the task. Do you need to collect any other form of data? How will you collect this? Develop and implement a plan for collecting this information. Ensure that you meet your own Data Protection and ethical requirements.*
Synthesis	*In order to find out the main impediments to the implementation of the video camera system in the above-mentioned places, the CEO asks you to write a short report (maximum 1-2 pages). Please note that this report will be submitted to the CEO and the other Departments involved, so you must avoid using legal language in excess.*
Reflections	*Please provide a reflective statement in your journal to summarise your answers to the questions below:* *1. What are the key problems to be overcome in this challenge?* *2. How did you organise the work involved in the investigation?* *3. How did you collect additional data? What worked well about this?* *4. What information gaps were still present at the end?* *5. How successful was the investigation process?*
Other notes	*Any other notes that teachers and students should be aware of when using this challenge.*

3. Act	
Solution Prototypes	*Prepare a complete legal report analyzing the legal consequences arising from the implementation of video surveillance systems in each of the areas proposed by the CEO. Keep in mind that the company is firmly convinced of the implementation of video cameras, hence the option of not installing the cameras is the least desired by the company.* *Therefore, you must assess the legal feasibility of such action. In order to achieve it, you must take into account:* • *Proportionality of the measure* • *Positioning of the cameras* • *Data Protection Impact Assessment* • *Processing principles involved* • *Necessary safety measures* • *Etc.*
Solution	*Please indicate your key recommendations to the CEO here:*
Implementation plan	*Please develop a plan for the implementation of the legal report.*
Evaluate	*Please develop a journal entry which answers the following questions:* *1. Among the measures you do propose to the company, which ones do you think will be the most rejected? Why?* *2. What were the strengths and weaknesses of your overall legal report?*
Other notes	*Any other notes that teachers and students should be aware of when using this challenge.*
4. Reflection and documentation	
Case notes	*Your notes and reflections on how this challenge could be developed in the future.*

Challenge Title: Responding to a Data Breach in a University	
Use Case Author	*Andrew Morris, Martin Maguire, Nathan Stuttard, Loughborough University*
Topic	*Privacy in Public Administration*
Overview	*You are the Academic Registrar at the University of Baloney.* *A number of students have complained to the Vice-Chancellor of the University which you represent. They are very unhappy that their marks have become public and are available to both fellow students and the general public.* *The VC has tasked you with trying to establish the source of the data breach. You have to carry out an investigation to find out how the breach has occurred, and which behavioural antecedents contributed to the data breach. You suspect that the data breach was malicious, not accidental but you cannot be certain.* *In the event that the breach was malicious, you are also determined to establish the motivation and causes for the breach.* *In the event that the breach was accidental and an 'honest mistake', you want to establish how this occurred and whether the member of staff knew* *what they had done but not "why".*
1. Engage	
Big idea	*Students' final exam marks have been published on Social Media with abuse from the author.*
Essential Question	*How should University staff act appropriately in order to deal with the breach and avoid major data breaches in future?*
Initial resources	*The following links show examples of data breaches that have taken place in universities: https://www.youtube.com/results?search_query=Data+breach+at+University* *https://www.youtube.com/watch?v=QclLzNd0EQg* *https://www.youtube.com/watch?v=g61BpB04xKc* *https://www.youtube.com/watch?v=L9TRbORKshU*
Guiding Questions	• *How would you go about investigating the breach?* • *Which members of staff would you involve in the investigation?* • *What do you think caused the breach?* • *How would you ensure that such a data breach cannot happen in future?* • *What other actions would you need to take? e.g. reporting the*

	event, making a public statement. *Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to develop a list of questions which break the challenge down into its constituent elements and manageable sections and to put these in a logical order.* *---* *Use this space to show how you will do this. And Leave space for the students to complete the questions. This box should be completed as a team by the students.*
Reflections	*Once the students have done this, encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge? How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process.*
Other notes	*None.*
2. Investigate	
Activity Description	*Students need to map out a process of investigation for answering the questions above.*
Resources	*Some helpful information that might help you to get started. http://www.lboro.ac.uk/admin/ar/policy/dpact/* *Other resources will include printed statements from people involved for analysis as part of the investigation. The stories in the statements may not match completely so the students will need to work out how to resolve the information. Other items might be IT reports showing an audit trail of user interactions with the University database to try and work out how the breach occurred.* *----* *Searching through the following journals and databases may also help: Behaviour and Information Technology, Information and Management, Science Direct, Scopus, Taylor and Francis, Journal of Business Research and Computers and Security. Using multiple keyword combinations will assist with this* *Encourage students to collect and use further resources to help them to address the question.*
Synthesis	*Students should prepare a PowerPoint presentation to synthesise their answer to the questions raised above.* *---* *Encourage students to summarise their answer.*
Reflections	*Encourage students to provide a reflection on the process.*

Other notes	*None.*
3. Act	
Solution Prototypes	*Each student group will provide a classroom briefing to fellow students to explain the outcome of their investigation and the implications that will follow. These will include:* *• The cause and source of the breach* *• The implications and how these will be handled* *• The nature of your investigation* *• Your recommendations to University Management as to how similar breaches will be avoided in the future.* *Based on a Behavioural rationale, your recommendations should be geared towards improving attitudes to data security and awareness of the implications of data breaches.*
Solution	*Please indicate your key recommendations to the University Management here.*
Implementation plan	*Please develop a plan for the implementation of the project.*
Evaluate	*Please address the following questions:* *1. What are the key challenges for your University in implementing the plan you identified?* *2. What were the strengths and weaknesses of your overall approach to the challenge?* *3. Were there any changes that could be made to University Policy?* *4. What did you learn from this whole process?*
Other notes	*None.*
4. Reflection and documentation	
Case notes	*Gather class feedback from students about their experience in attending the class and conducting the exercise.* *If you were to run this challenge again with a group of learners, how would you change it?*

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

ADRIÁN PALMA ORTIGOSA – Assistant Researcher at Seville University

ALEX NUNN – Professor of Global Political Economy at Derby University, member of the Scientific Committee of EJPLT

ANDREW MORRIS – BSc in Psychology, MSc in Ergonomics, Ph.D. in Mechanical Engineering at Loughborough University, member of the Scientific Committee of EJPLT

AURA TARDIA – Project Manager at RE:Lab, member of the Editorial Team of EJPLT

DAVIDE BORELLI – Ph.D. in Law at Suor orsola Benincasa University of Naples, Tech/-Digital & Data Lawyer (Manager) at PricewaterhouseCoopers Legal United Kingdom, and Fellow at the International Association of Privacy Professionals (IAPP)

ELISA LANDINI – Project Manager at RE:Lab

ERION MURATI – Ph.D Candidate at Hamburg University

FAUSTA SCIA – Researcher at Federico II University of Naples

FRANCESCO CIRILLO – Ph.D. (c) in Law and Cognitive Neuroscience at Unicusano

ILARIA AMELIA CAGGIANO – Full Professor of Private Law at Suor Orsola Benincasa University of Naples, Vice editor in chief of EJPLT

LIVIA AULINO – Ph.D. (c) in Law at Suor orsola Benincasa University of Naples

LUCILLA GATT – Full Professor of Civil Law at Suor orsola Benincasa University of Naples, Director of EJPLT

MANJOLA HËNKOJA – Graduated master's Economics at the University of Tirana

MARÍA BOCIO JARAMILLO – Assistant Researcher at Seville University

MARIA CRISTINA GAETA – Postdoctoral Research Fellow in Law at Suor Orsola Benincasa University of Naples, Ph.D. in Law at Federico II University of Naples, Coordinator of the Editorial Team of EJPLT

MARINÍ GAIA CHIACCHIO – Avvocato at the Court of Naples

MARIO RENNA – Postdoctoral Research Fellow in Law at Roma Tre University

MARIO TRIGGIANI – Teaching assistant in Law at Suor orsola Benincasa University of Naples

MARTIN MAGUIRE – BSc in Computer Studies and MSc in Ergonomics at Loughbor-

ough University, Ph. D. in Human-computer interaction at Leicester Polytechnic, member of the Referees Committee of EJPLT

NATHAN STUTTARD – BSc and MSc in Psychology at University of Nottingham

NOEL ARMAS CASTILLA – Ph.D. (c) in Law at Seville University, member of the Editorial Team

ROBERTO MONTANARI – Co-founder and Head of R&D at RE:Lab, Professor of Interaction Design at Suor Orsola Benincasa University of Naples, member of the Scientific Committee of EJPLT

SARA LORENZO CABRERA – Professor of Civil Law at Universidad de La Laguna, member of the Editorial Team

SARA SALERI, Project Manager at RE:Lab

TOMMASO EDOARDO FROSINI – Director of the Law Department and Full Professor of Constitutional Law at Suor Orosla Benincasa Universty of Naples