Instituto Hermes
Derechos de ciudadanía digital

El Dato: Su propiedad e intermediación

Instituto Hermes, derechos digitales

Contenidos

Los servicios digitales que utilizamos cada día sin coste alguno (Google, Facebook, Zoom...) recopilan datos personales y de nuestro comportamiento para explotarlos y sacar beneficio de ellos. No tenemos por qué renunciar a estos servicios, pero es importante que sepamos que gracias a los datos que les proporcionamos y a los algoritmos que sus sistemas utilizan, estas empresas pueden ofrecernos mejores servicios, pero también manipularnos.

Tras Internet y la eclosión de modelos de negocio basados en los datos digitales de los usuarios, hemos asistido a la creación de un oligopolio tecnológico que abre lo que muchos han llamado «capitalismo de vigilancia». Nuestros propios actos producen información que, una vez procesada, permite influir en nuestro comportamiento, anticipando nuestros deseos y condicionándolos. Si en el ámbito del mercado ha dado paso al «capitalismo de vigilancia», su impacto en el espacio social no es menos inquietante. La posibilidad de incidir en el comportamiento social y político es ya un hecho aceptado. Los datos, también tienen efecto en la democracia, en la calidad de las conversaciones, en el grado de crispación y cohesión de un país.

Sentimos que devoran nuestros datos...

¿es posible revertir o limitar esta situación?

#1 PUNTO DE PARTIDA

Nuestra sociedad sufre de tres afecciones en cuanto al uso de los datos que se retroalimentan entre sí: Confusión; Desconocimiento; Influencia.

Confusión sobre el significado, valor y uso de los datos. Entre dato individual y colectivo, uso público y uso privado, interés particular e interés general.

Desconocimiento sobre cómo se produce la captura de los datos a través de dispositivos electrónicos y servicios: cesión consciente e inconsciente.

Influencia de la centralización y manejo de datos en la esfera pública. El uso que hacen de los datos las empresas que capturan grandes cantidades de ellos impacta en la calidad de las democracias y la pérdida de diversidad en la conversación; produce polarización, radicalización, aislamiento social, desgaste y erosión de la convivencia, y desconfianza hacia las las instituciones del Estado.

Los trabajos del grupo han intentado dar respuesta a las siguientes preguntas, conscientes del nivel de confusión que opera en el espacio público en torno al dato, su valor y su explotación.

1. ¿Qué es el dato?
2. ¿Para qué se usan los datos?
3. ¿Cuáles son los problemas de privacidad?

El propósito de nuestros trabajos es identificar el problema, su alcance y elaborar propuestas de actuación, teniendo en cuenta, que como todo proyecto del Instituto Hermes, los resultados deben estar orientados a transformar. Es por ello que aspiramos a,

- Aportar luz a la cuestión de los datos, definir de forma clara los términos clave para contribuir reducir los malentendidos.
- Concienciar a la población sobre la importancia de la privacidad y los datos a nivel individual en su relación con empresas e instituciones públicas.
- Proponer a los representantes políticos ámbitos de actuación.

#2 ¿QUÉ ES EL DATO?

Desde el punto de vista de los derechos digitales, cuando hablamos de dato nos referimos a tres tipos de información diferentes:

1. El conjunto de **«datos de carácter personal»** o «datos personales».
2. Los datos de **«carácter no personal»** resultantes de la actividad humana.
3. Los datos **producidos y recogidos por máquinas y sistemas de interacción** física sobre su propio funcionamiento, sobre el uso que reciben por el conjunto de sus usuarios, o como resultado de la función para la que fueron creadas.

Las fronteras entre estas tres categorías no son infranqueables:

- Los datos personales pueden ser agregados y anonimizados, pero ...
- ... Algunos conjuntos de datos de carácter no personal pueden utilizarse para **inferir comportamientos** o **información** personal,
- ... Y por supuesto, los datos recogidos por máquinas pueden llegar a tener una traducción casi inmediata en términos de **control**. No es lo mismo tomar datos metereológicos que datos de conducción. Si tenemos el modelo del vehículo y las coordenadas de los extremos de sus itinerarios más habituales, asociar los datos a una identidad será prácticamente inmediato.

#3 EL VALOR DEL DATO INDIVIDUAL

Es peligroso despertar en los usuarios la ilusión de una retribución monetaria individualizada por el uso de sus datos.

Lo cierto es que los datos individuales obtenidos de la utilización de los grandes servicios digitales de cada consumidor, aisladamente considerados, carecen de valor significativo pues en solitario no alcanzan el umbral necesario para su monetización. El beneficio que obtienen las empresas proviene de su agregación y comparación con otros datos de otros usuarios, que es lo que permite extraer conclusiones valiosas para la comercialización y el perfilado. **El valor depende por tanto, de la capacidad del agregador para, mediante el uso de algoritmos o Inteligencia Artificial, convertirlos en herramientas predictivas** de nuestros deseos o comportamiento. Incluso puede defenderse que el valor lo obtiene el propio usuario: por ejemplo, un usuario de Spotify consigue mejores recomendaciones musicales precisamente porque sus datos, junto con los de los demás usuarios del servicio, permiten identificar qué canciones potencialmente le puedan gustar. Por tanto, lo trascendente no es que se devuelva el valor singular a cada usuario, sino que **la obtención de los datos y su uso sean respetuosos con los derechos fundamentales**. Volviendo al ejemplo, lo que no se podría permitir es que las recomendaciones estuvieran sesgadas por aquellos productores que paguen a Spotify en lugar de por las elecciones y gustos musicales del usuario.

La cuestión fundamental en el plantamiento sobre la explotación del dato es de **carácter ético** y tiene que ver con la aceptación de la **mercantilización de la intimidad de las personas**. Si les damos valor individual a los datos, estamos **amparando su venta y su comercialización**, que alguien pueda pagar por la privacidad de otro. Y del mismo modo que no permitimos que se comercie con un órgano de nuestro cuerpo, deberíamos plantearnos si la intimidad es renunciable y vendible, si es algo que se debe someter al comercio de los hombres.

Un debate de más calado que el valor individual del dato, es el del **valor social de los datos agregados** para fines de interés público. Por ejemplo, los datos de uso de teléfonos móviles, agregados y anonimizados, pueden ser de enorme utilidad para mejorar la planificacIón del transporte público y privado urbano e interurbano, conocer la efectividad de las restricciones pandémicas o fijar las tasas municipales de espacios publicitarios. Igualmente los datos de consumo de electricidad o de agua, o de uso de las tarjetas de crédito, e incluso los datos de salud, anonimizados, lo son para el desarrrollo científico. Consideramos que la cuestión a dilucidar debería ser:

¿Quién, cómo y a qué precio debe poder acceder a esos datos?

#4 USO PÚBLICO DE LOS DATOS

Vamos viendo así que existe un «desdoblamiento de la naturaleza del dato», el dato particular, protegido por las leyes de privacidad y el dato para uso público e industrial, anonimizado. En este sentido, las instituciones europeas consideran estratégico la creación de un espacio europeo de datos para uso industrial, que permita a la industria la explotación conjunta de grandes masas de datos anonimizados con el objetivo de acelerar la competitividad de las empresas europeas en nueve sectores identificados como críticos. Entre ellos: transporte/automoción, salud, energía y agricultura, como medio para fomentar un mayor intercambio de datos industriales.

Según las conclusiones de la cumbre del Consejo Europeo de octubre de 2020, los líderes de la UE están decididos a presionar a la Comisión para que avance rápidamente en el establecimiento de espacios de datos sectoriales tal como describe la «Estrategia de Datos» en actual elaboración. Su objetivo es hacer que las industrias de la UE sean más competitivas a escala mundial y aumentar su autonomía. Para apoyar el establecimiento de tales espacios, la Comisión espera avanzar en paralelo la **«Ley de Gobernanza de Datos»** propuesta el año pasado con el fin de proporcionar el marco para fomentar un mercado único de datos dentro de la Unión.

Se piensa por ejemplo en la «conducción cooperativa» sin la que la industria automotriz europea no cree que pueda competir con los fabricantes asiáticos y estadounidenses. Se trataría de compartir todos los datos recogidos por la industria del uso de sus propios vehículos por particulares y los datos de tráfico generados por los sistemas de vigilancia de los estados para alimentar las IAs que guiarán la conducción autónoma en el futuro inmediato.

La estrategia de la Comisión tiene como objetivo garantizar que Europa aproveche el potencial que ofrecen estos desarrollos convirtiéndose en un «modelo a seguir». Para lograrlo, establece un **espacio de datos cooperativizados**, en beneficio de administraciones públicas, investigadores, empresas y ciudadanos; **«El principio subyacente es poner los datos a disposición de todos»**.

De esta forma, **los datos serían una riqueza común europea al servicio del I+D y la competitividad de todas las empresas**.

El modelo hacia el que se encamina Europa está alineado con estrategias a nivel nacional ya experimentadas en países como Corea del Sur. De características poblacionales muy similares a España, Corea optó a finales de la década de los 90 por un modelo de desarrollo económico basado en el despliegue de Internet y el impulso de la economía digital. Hoy, su sistema de datos abiertos está reconocido como buena práctica a nivel global, permitiendo que el conjunto de la sociedad se beneficie de la gestión de los datos de los ciudadanos procedentes de la interacción de estos con servicios públicos y privados.

Este uso público del dato abre una nueva perspectiva en la idea de explotación privada de los datos. Y en un segundo momento nos permitiría adentrarnos en cuestiones de mayor calado, repercusión social e incluso de retribución económica.

> *¿Podríamos pensar en la creación de nuevos impuestos a las empresas que utilizan datos públicos para el desarrollo de su actividad económica? ¿En una suerte de «**dividendo digital**» que colectivamente, a través del estado, podamos reclamar a las empresas que hacen negocio a partir de los datos cedidos por los ciudadanos?*

En otro plano, las reacciones en contra de los abusos de las empresas han alcanzado un cierto nivel de relevancia. Según datos de Eurostat (2019), uno de cada cuatro ciudadanos de la Unión Europea de entre 16 y 74 años afirma haber evitado proporcionar información personal en redes sociales o profesionales por motivos de seguridad. En España, el porcentaje de ciudadanos que aseguraron haber evitado compartir información personal en redes sociales por considerar que existían riesgos de seguridad era del 34%.

También empiezan a ser recurrentes las quejas contra los contratos de adhesión, dado que:

- Son el grueso de los contratos que se firman en Internet.
- Los derechos de los consumidores/usuarios se ven comprometidos. El acceso al servicio se ve condicionado por la aceptación total de las cláusulas del contrato; no existe comprobación de lectura, entendimiento y aceptación efectiva del contrato; los usuarios/consumidores desconocen los derechos y las obligaciones a las que quedan vinculados por la aceptación del contrato.
- Entre las cláusulas de obligada aceptación figuran cuestiones relativas a la aceptación de recogida de datos y su proceso, no siendo todos los datos solicitados estrictamente necesarios para el desarrollo del servicio.

#5 GARANTÍAS PARA LOS USUARIOS EN EL ENTORNO DIGITAL

PROTECCIÓN EFECTIVA DEL DATO vs. SOBREPROTECCIÓN FORMAL

La regulación a tanto a nivel de la Unión Europea como de España ha procurado crear un marco regulatorio exhaustivo en cuanto al nivel de exigencia a empresas y administraciones públicas. Sin embargo, en la práctica cotidiana se dan situaciones que nos obligan a cuestionarnos si la sobreprotección formal no acaba erosionando la protección efectiva del dato, pues ciertamente, está generando algunos efectos contraproducentes.

Todos estamos hartos de tener que dar nuestro consentimiento a la utilización de cookies o de firmar apresuradamente consentimientos para el uso de datos simplemente porque queremos acceder a una información en una página web o a un servicio. Eso trivializa el consentimiento y acaba provocando que no le demos valor.

Lo mismo ocurre con las sanciones. La severidad y el rigor de la normativa europea de protección de datos ha impulsado una situación incómoda, si no indeseable. El exagerado importe de las multas que se pueden imponer, y la aparente objetivación de los motivos para imponerlas, se está convirtiendo en un elemento disuasorio a la innovación en muchos terrenos. Casi ningún delegado de protección de datos se atreve a dar su visto bueno a una innovación por el riesgo de que acabe siendo considerada una infracción. Es tal el temor, que la mejor respuesta es siempre no. Esto se ha hecho más preocupante con la reciente decisión de la AEPD de no contestar en lo sucesivo a consultas sobre la aplicación de la Ley.

Es cierto que esto es congruente con el principio del RGPD de que corresponde al responsable del tratamiento la evaluación de su impacto y la aplicación del ***privacy by design***. Pero como el coste del error puede ser de tal magnitud, y los márgenes interpretativos en terrenos de permanente evolución tecnológica son tan amplios, el ejercicio desmesurado de la potestad sancionadora puede provocar un efecto de involución tecnológica que sitúe a Europa en una posición de franca desventaja frente a otros países, que ya hoy cuentan con una tecnología más avanzada.

Basta leer cualquier contrato de suministro o de servicio para comprobar que una buena parte de su contenido se refiere siempre a los consentimientos de protección de datos.

¿Tiene lógica y tiene efecto alguno esa sobre información?

¿Nos protege efectivamente de intromisiones graves en nuestros derechos?

LOS DATOS Y LA CARRERA TECNOLÓGICA

En relación a los datos y la carrera tecnológica, la UE promueve la Ley de gobernanza de datos (DGA) cuyo objetivo es crear nuevas reglas sobre neutralidad de los mercados de datos y facilitar la reutilización de datos generados por el sector público. Dicho en pocas palabras: el objetivo de la DGA es facilitar el acopio de datos por empresas emergentes para impulsar el desarrollo de la IA en la UE creando «un Schengen de los datos». Entre los elementos más interesantes de la posición del Parlamento destacamos:

- Los **organismos del sector público deberían evitar la celebración de acuerdos que creen derechos exclusivos para la reutilización de ciertos datos**. En todo caso, afirman los eurodiputados, los acuerdos exclusivos deberían tener un período máximo de 12 meses antes de liberarse al dominio público y quedar en manos de la ciudadanía y las PYMEs.

- Los **datos sensibles del sector público pueden transferirse a terceros países solo cuando se benefician de un nivel de protección similar al de la UE**. La Comisión declarará si un tercer país proporciona dicha protección mediante un acto delegado que permita al Parlamento opinar sobre la decisión.

- La **donación de datos de los ciudadanos con fines altruistas** («como la investigación científica, la atención médica, la lucha contra el cambio climático o la mejora de la movilidad») no solo exigirá consentimiento informado sino que deberá articularse a través de organizaciones reconocidas por la Unión que inscribirán los datos en un registro específico.

La Unión Europea tiene claro que si no queremos quedarnos atrás en la carrera tecnológica, en un momento en el que este retraso sería trágico para la economía, **debemos articular el marco legal para que cantidades masivas de datos puedan ser utilizadas por la industria sin dejar de respetar los derechos fundamentales**.

Las voces más críticas con la explotación de los datos de los usuarios ven con mejores ojos a las empresa europeas emergentes y a las PYMEs, supuestas beneficiarias de la nueva política de datos, que a las grandes tecnológicas norteamericanas. Pero hacer políticas separadas para unas y otras en mitad de una guerra comercial de equilibrios imposibles lo convierte en todo un reto.

#6 ALGUNAS CONCLUSIONES

Europa, y con ella España, no pueden quedar atrás en la carrera de la Inteligencia Artificial y la interpretación de «Big Data». Estas tecnologías necesitan datos en cantidades masivas.

Los beneficios de esta transformación, tanto para nuestras economías como para nuestra vida diaria, se verán eclipsados si el uso de los datos no sitúa los intereses de la persona en primer lugar.

Encontrar el **equilibrio entre los datos como valor económico y como valor jurídico protegible** es uno de los mayores retos que tenemos.

Los ciudadanos solo confiarán y harán suyas las innovaciones basadas en los datos si confían en que todo intercambio de datos personales en la UE estará sujeto al pleno respeto de sus estrictas normas en materia de protección de datos.

La privacidad no está en venta, mucho menos se puede robar.

A día de hoy, **el dato individual tiene valor pero no precio**.

- Existen algunas excepciones: aquellas en las que se establece un intercambio claro entre los datos personales del usuario y un servicio, producto o descuento en el mismo.
- El valor del dato individual también se evidencia en que un uso malicioso del mismo tiene consecuencias negativas para los derechos fundamentales.

Es necesario **reivindicar el derecho a la privacidad**. El comercio de datos –es decir, el lucro a través del tratamiento y la explotación de los datos personales de los usuarios– sin conocimiento y por tanto sin consentimiento del usuario, debe ser prohibido.

Necesitamos **transparencia en la captura de datos**. No puede ser decisión exclusiva de la empresa, por ejemplo, que haya cookies técnicas «necesarias» que no se puedan deshabilitar.

Necesitamos **reglas** del juego **claras y justas para todos**. La innovación se está viendo afectada por el temor a sanciones económicas cuya argumentación varía según el caso, mientras que los grandes infractores quedan impunes.

Para generar confianza y seguridad en los ciudadanos a la hora de proporcionar sus datos personales, es necesario **sensibilizar socialmente respecto a la importancia de la privacidad**, así como crear y extender una cultura de protección de datos.

Del uso del dato individual: Consecuencias individuales para el ciudadano del análisis de sus datos

El uso de sistemas inteligentes de predicción del comportamiento destinados a influir en el usuario y condicionar sus decisiones tiene consecuencias para los derechos fundamentales que deben ser consideradas por el regulador, destacando:

- Polarización social
- Odio online
- Crecimiento de las teorías conspirativas
- Oportunidad de desestabilización para agentes externos
- Sesgos informativos
- Denegación de servicios (como créditos bancarios), pérdida de oportunidades laborales o aumento de primas de seguros basados en el comportamiento previo del usuario que es categorizado por sistemas automatizados.

El ejemplo del «Sistema de crédito social» chino debe advertirnos sobre el peligro que el registro y análisis del comportamiento tiene para los derechos civiles y las libertades públicas.

#7 PROPUESTAS

1. De la obtención del dato individual: Transparencia y control

Propuesta 1 -- Propiciar las tecnologías que garantizan una mayor seguridad y privacidad en el uso de los datos

Propuesta 2 -- Centro Nacional del Dato: Dentro de la Comisión Nacional de los Mercados y la Competencia (CNMC), cuya finalidad es promover y defender el buen funcionamiento de todos los mercados en interés de los consumidores y de las empresas, se hace necesaria la **creación del Centro Nacional del Dato** como Autoridad Administrativa Independiente Reguladora del Dato. Se trataría del ente regulador del mercado del Dato, encargado de controlar dicha actividad y, en consecuencia, regular un mercado respecto del que hay que acabar con su falta de transparencia. Su actuación alcanzaría a todos los mercados y a todos los entes reguladores.

1. Si un usuario web acepta las **cookies**, tal actividad debería pasar automáticamente al Centro Nacional del Dato para su constancia y, por consiguiente, éste, como ente regulador de dicho mercado, poner en marcha los mecanismos de su supervisión, análisis y regulación.

2. El Centro Nacional del Dato debería asimismo facilitar a los usuarios que hemos cedido nuestros **datos** (la mayoría de las veces involuntariamente a través de la aceptación de las coockies) **la posibilidad de consultar cuáles son todos los datos de los que, sobre nosotros, disponen todas y cada una de las empresas que mercadean con ellos**. Siendo ésta una de las formas de resarcir a la ciudadanía por tal utilización mercantil.

Propuesta 3 -- Registro del Tráfico del Dato
Consiguiente necesidad de creación del Registro del Tráfico del Dato, toda vez que si una empresa puede captar los datos de los usuarios web, la Administración debería igualmente estar legitimada para tener constancia y registrar ese tráfico. Por lo que el Tráfico del Dato con la Administración se convierte en obligatorio.

#7 PROPUESTAS

1. De la obtención del dato individual: Transparencia y control

Propuesta 4 -- Cookies
Regulación para la unificación de los términos y condiciones asociados a las cookies y la imposición de un único modelo para todas las webs.

1. Acabar definitivamente con el sistema actual y proponer uno más claro y transparente para la ciudadanía, y que se establezca primando el beneficio de los ciudadanos al de las empresas -de ahí la importancia del Centro Nacional del Dato como entre regulador.
2. La aceptación, en su caso, de las cookies debería de ir precedida de una muy breve y clara explicación de qué es lo que se acepta y a cambio de qué, con letra también clara y de tamaño adecuado, huyendo de la actual letra minúscula y de la redacción confusa, extensa, más propia de los injustos contratos de adhesión.
3. La explicación y sus requisitos serían obligatorios. Debe ser posible rechazar todas las cookies. **En ningún caso la prestación del servicio puede verse condicionada a su aceptación**.

Propuesta 5 -- Registro Oficial de acceso público
Organización de un registro oficial de acceso público de todos los contratos de adhesión, términos y condiciones del servicio de cualquier servicio online, sin importar su origen, que facture más de X € /año.

Propuesta 6 -- Punto Neutro Judicial del Dato
Creación del Punto Neutro Judicial del Dato, a efectos de que los Jueces y Tribunales puedan acceder justificadamente a dichos datos, sin tener que pedir comisiones rogatorias a EEUU u otros países extracomunitarios.

Propuesta 7 -- Creación de la Policía del Dato
Policía administrativa que ejerce el control del dato, así como del acceso al punto neutro del dato por Jueces y Tribunales justificadamente.

#7 PROPUESTAS

2. Del uso agregado de los datos y su monetización

El beneficio empresarial derivado de la explotación comercial de datos personales debe ser transparente, estar controlada y ser regulada.

Propuesta -- Dividendo digital

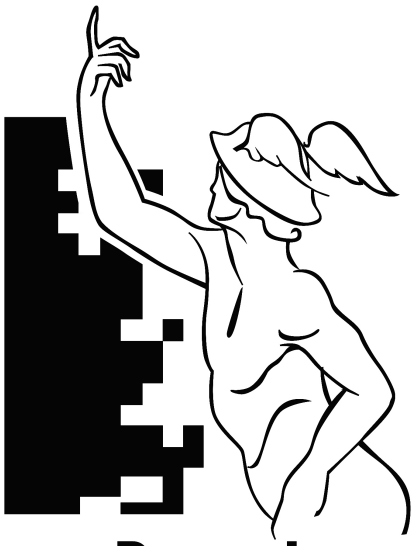
Creación de un **impuesto para las empresas que utilizan los datos de los usuarios y generan beneficios** de algún tipo (económicos o de cualquier otra naturaleza), datos obtenidos de forma poco o nada transparente y por mecanismos semejantes a los del contrato de adhesión. El objetivo es que ese beneficio obtenido repercuta en los ciudadanos (por ejemplo, mejoras económicas en el sistema de pensiones, en la protección del medio ambiente, en la calidad de vida, o en cualquier otro sector de relevancia para la ciudadanía).

3. Concienciación

Propuestas

Implicar a instituciones públicas y organizaciones privadas en campañas de sensibilización masivas.

Incluir f**ormación en privacidad y protección de datos en los currículos** de secundaria obligatoria, Formación Profesional y grados superiores.



Instituto Hermes

Derechos de ciudadanía digital