ie UNIVERSITY
LAW SCHOOL

ECIJA

# OBSERVATORIO DE DERECHO DIGITAL IE – ECIJA

Informe del Focus Group – DATA GOVERNANCE

https://www.ie.edu/odigitallaw/

## Introducción

El pasado 12 de abril de 2023 tuvo lugar la sesión de trabajo o focus group sobre *data governance* y protección de datos en el marco de las actividades del Observatorio de Derecho Digital IE-ECIJA. En esta ocasión, el objetivo de los participantes fue analizar y debatir el concepto y dimensiones de los sistemas de gobernanza del dato y algunas las principales implicaciones, retos y tendencias en materia de privacidad.

Los participantes del focus group, miembros de los equipos jurídicos y de privacidad de importantes empresas pertenecientes a diversos sectores cuyo factor común es la relevancia de los datos presente en su actividad, compartieron sus experiencias, conocimientos y opiniones sobre los sistemas de *data governance* y los principales retos y necesidades/oportunidades que identifican desde sus respectivas posiciones.

El presente informe es el resultado de todo lo compartido durante la interesante sesión de trabajo.

---

## Sistemas de gobernanza del dato o *data governance*. Concepto

Se trata del conjunto de mecanismos y estructuras corporativas orientados a controlar y gestionar, con un objetivo último comercial, toda la información del negocio, considerando como parte de este todo tipo de datos, no sólo los de carácter personal. Comprende, por tanto: **procedimientos, personas e infraestructuras**.

En términos generales, su objetivo es asegurar que la información corporativa alcanza altos estándares de disponibilidad, integridad, seguridad, relevancia y usabilidad para permitir la toma de decisiones, así como una gestión de la información coherente con la estrategia de la organización.

En palabras de The Global Data Management Community (DAMA), "*es el ejercicio de autoridad y control (planificación, monitorización y aplicación) sobre la gestión de los datos. La función del Data Governance guía el resto de las funciones del Data Management*".

No resulta difícil entender la razón por la que cada vez hay más empresas inmersas en la revisión de sus estructuras y procesos para crear su sistema de gobernanza de los datos.

Los datos son un activo intangible esencial para cualquier empresa que permite desde lo más básico, la adecuada gestión del negocio y una toma de decisiones informada, hasta cuestiones estratégicas de mayor madurez como procesos de transformación digital o estrategias de la tan ansiada monetización de la información.

Podemos señalar como razones para la implementación de un sistema de *data governance*, que:

- A través de estos sistemas se establecen los parámetros necesarios para la gestión y el uso de los datos en una organización, mejorando así su accesibilidad;
- Asimismo, contribuyen a un nivel adecuado de cumplimiento normativo, especialmente en términos de privacidad y confidencialidad de la información;
- Mejoran la flexibilidad de la empresa, así como su eficacia y eficiencia en términos de costes;
- Coadyuvan a la reducción de riesgos de diversa naturaleza (estratégicos, relacionados con la continuidad de negocio, legales, reputacionales, etc.);
- Mejoran la calidad de la información que se maneja;
- Sirven de apoyo a las estrategias generales del modelo de negocio en cuestión;
- Permiten la gestión de la información de forma que contribuya a la satisfacción y fidelización del cliente interno y externo;
- Agregan y protegen el valor del activo intangible;

Adicionalmente, y dado que el volumen de datos que manejan las empresas es cada vez mayor, carecer de estrategias de *data management* y *data governance* conlleva desorganización y caos respecto de la información y priva a las organizaciones de los beneficios de este sistema de gestión.

**¿Qué se requiere para poner en marcha un sistema *data governance*?**

- En primer lugar, es necesario identificar cuál o cuáles son los objetivos de cada empresa al implementar su sistema de gobierno de la información. Solo así será posible definir el alcance, los sistemas e infraestructura necesarias y otras necesidades. Si bien es cierto que hay objetivos comunes a cualquier sistema de *data governance*, cada organización tendrá, además, objetivos propios alineados con su estrategia empresarial y comercial a fin de que la gestión de la información contribuya de forma sustancial a su consecución.

- Como siguiente paso, se requiere el inventario de los activos. Deben identificarse las bases de datos presentes en la organización, así como su origen, sistemas información involucrados, usos, finalidades, etc. Se requiere un conocimiento completo del ciclo de vida de los datos a fin de poder intervenir sobre él en su mejora.

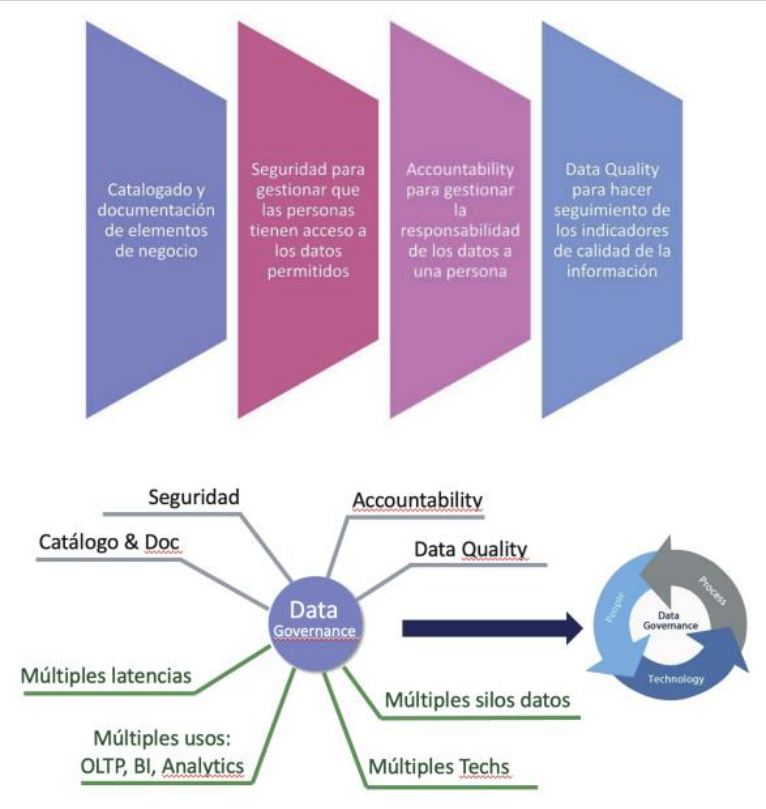
- Políticas, procesos y roles. Un sistema de *data governance* requiere de un conjunto de reglas y procedimientos bien definidos. Unos, diseñados para guiar el tratamiento efectivo de la información y sus particularidades, como, por ejemplo, la captación de datos, su uso, conservación, seguridad y procesos de anonimización o transformación. Otros, como directrices o *guidelines*, que serán encargadas de hacer realidad las reglas anteriores en la organización a través de las herramientas y personas involucradas. De nuevo, todas las políticas anteriores deben estar alineadas con los objetivos estratégicos de la organización, sólo así existirá coherencia entre las diferentes directrices y la gestión de la información contribuirá de forma significativa a la contribución de los objetivos de la empresa.

- Para el correcto funcionamiento del sistema es fundamental un equipo humano con roles y responsabilidades bien definidas y acordes a sus capacitaciones y experiencia. La composición variará de una empresa a otra en atención a sus características y necesidades particulares, siendo habitual que formen parte de ese equipo humano posiciones como el *Chief Data Officer (CDO), Chief Information Officer (CISO), Chief Privacy Officer (CPO)*.

- Son necesarias herramientas tecnológicas y una arquitectura que sustenten el sistema de gobernanza, permitiendo el almacenamiento y gestión de la información en condiciones de seguridad y de forma que permita la gestión del ciclo de vida completo de los datos de la organización. Los sistemas de gestión de la información son clave para permitir una gestión de los datos ordenada, ágil y flexible. Asimismo, serán la clave para mejorar su calidad, optimizar su uso y permitir su reutilización. Se requiere, por tanto, su identificación y detalle para, posteriormente, verificar si la estructura o aplicativos seleccionados permiten a la organización una gestión de la información acorde con las finalidades y procedimientos definidos.

- Será necesario el establecimiento de un sistema de seguimiento y control para, por un lado, verificar la implementación efectiva de las políticas diseñadas y, por otro, ser capaz de medir el impacto que la implementación del sistema de *data governance* genera en nuestra organización para lo que será necesario determinar los ratios o KPIs de relevancia en cada organización.

- Como en cualquier proceso de mejora de estas características hay un factor cultural enormemente relevante que no debe dejarse de lado. La formación y concienciación respecto del valor del activo que es la información contribuirán a que los miembros de la empresa entiendan y coadyuven a la puesta en marcha y mantenimiento del sistema.



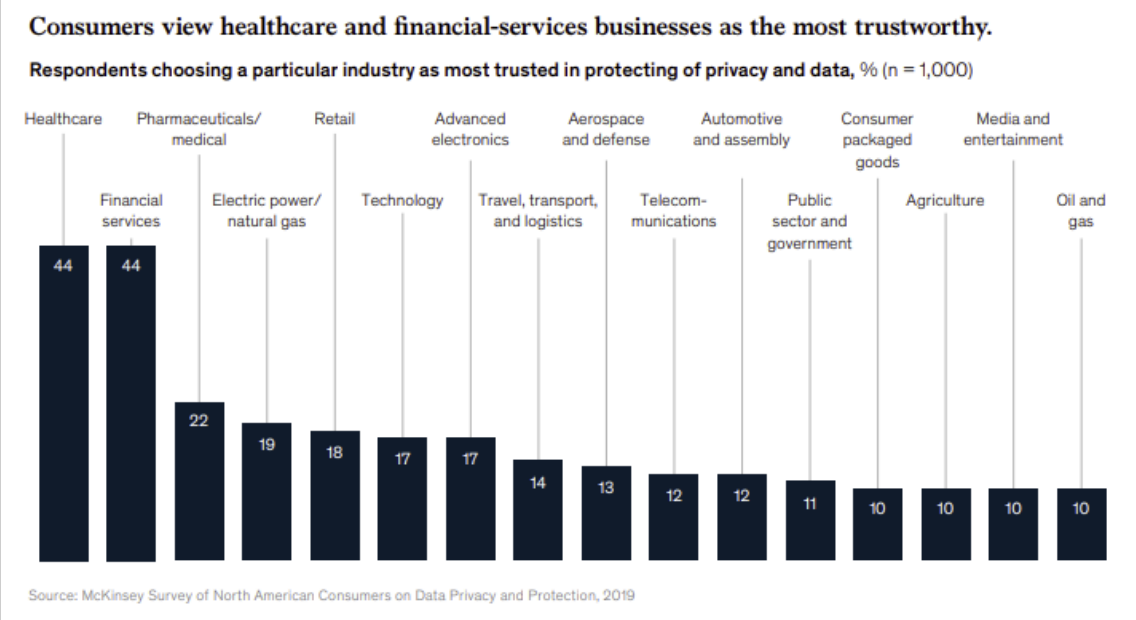

Fuente: Graph Everywhere

Si bien es cierto que resulta complejo acceder a información solvente y actualizada que ayude a dimensionar la inversión o apuesta del sector empresarial en este tipo de sistemas, no puede negarse que, en los últimos años, la relevancia y beneficios de disponer de un adecuado sistema de *data governance* no ha dejado crecer, particularmente sobre la base de varios factores:

- ✓ El aumento de la cantidad de datos que las empresas son capaces de generar. Tanto es así que para el año 2025 la Unión Europea estima en un 530% el aumento del volumen mundial de datos (de 33 zetabytes en 2018 a 175 zetabytes).

- ✓ La preocupación o interés de las empresas de todo el mundo por explotar la información de forma eficiente y monetizar su valor.
- ✓ El aumento de la regulación cuyos objetivos son tanto la mejora de los riesgos relacionados con la información como la creación de marcos legales que impulsen y fomenten la economía de los datos, como es el caso de la *Data Governance Act*[1] (DGA), propuesta legislativa de la Comisión Europea cuyo objetivo es impulsar la economía de los datos, fomentando el intercambio, circulación y disponibilidad de los datos entre el sector público y privado, cuyas obligaciones serán exigibles a partir de septiembre de 2023.

Asimismo, hay ciertos sectores especialmente receptivos a la adopción de un sistema de *data governance*, bien sea por el volumen de datos que manejan y/o por la sensibilidad de estos, así como por el marco regulatorio al que se encuentran sometidos – como el sector tecnológico, el de la banca o la salud –.




Fuente: McKinsey

[1] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)

No obstante, en Europa existe un marco regulatorio de alto impacto y común a todas las empresas, para cuyo cumplimiento resulta de suma utilidad disponer de un sistema de *data governance*, y es el Reglamento Europeo de Protección de Datos[2]. De ahí que las cuestiones relacionadas con la privacidad tengan una especial relevancia al hablar de gobernanza de los datos y que fueran diversas cuestiones relacionadas con ella las que fueron tratadas en el marco del *focus group* que da origen al presente informe.

**La monetización del activo**

Cuando hablamos de gestión y explotación de la información, hay diversas cuestiones que centran la atención y preocupación de las empresas; entre ellas, la monetización de dicha información y la presencia de principios éticos en el marco de su tratamiento.

En el marco de una economía como la actual, basada en los datos, es evidente que el objetivo principal de cualquier empresa en relación con la información de la que dispone es de carácter comercial y económico. Los datos son uno de los activos intangibles de mayor valor en el caso de muchas empresas y los esfuerzos de estas se concentran en incrementar su valor y monetizarlo. La monetización de esta información puede ser de carácter directo o indirecto.

La capacidad de alcanzar la monetización indirecta de la información está íntimamente ligada a su capacidad de contribuir a los objetivos estratégicos de la empresa y las posibilidades en este sentido son amplias, entre ellas:

- Una adecuada gestión de la información contribuye positivamente a la mejora en la toma de decisiones de tal forma que estas den lugar a acciones que mejoren la eficiencia de la organización;
- Asimismo, permite un conocimiento más amplio del *target* que facilitará la mejora del producto o servicio;
- Contribuye a un mejor direccionamiento de la estrategia comercial de la empresa y diferenciarse de las empresas competidoras;
- Coadyuva a la reducción de los costes y riesgos empresariales;
- E incluso, puede manifestarse en términos de reputación corporativa y generación de confianza.

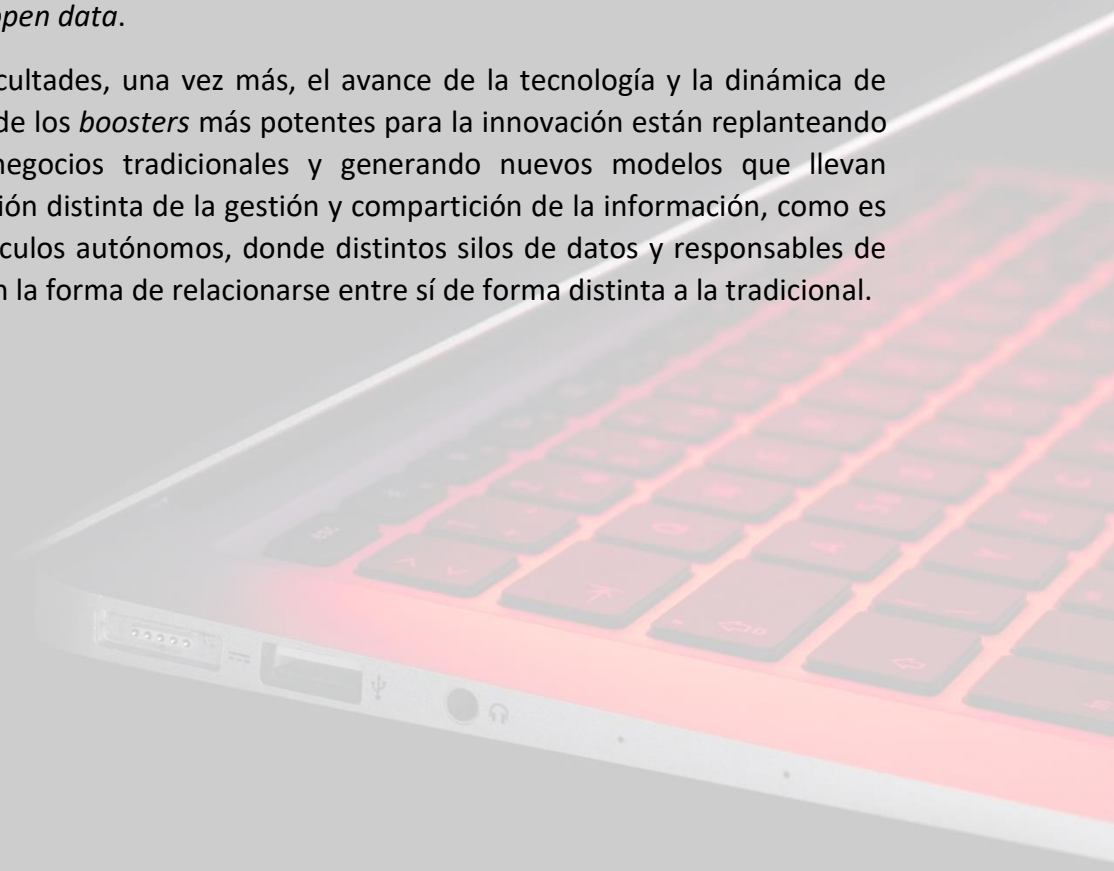
[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

No obstante, las fórmulas de monetización directa de la información, esto es, aquellas capaces de reportar un beneficio económico directo, son las que más llaman la atención del sector empresarial. Ahora bien, cuando hay datos de carácter personal implicados en estas operaciones, los principios que impone el RGPD en relación con la necesidad de contar con consentimiento específicos para cada finalidad y el principio de minimización de los datos, limitan las posibilidades, especialmente si estas involucran a otras empresas o *stakeholders.*

Más allá de operaciones como la venta del activo intangible asociada a una empresa o rama de actividad, la posibilidad de vender o licenciar datos encuentra también barreras regulatorias. De ahí que las técnicas de anonimización, seudonimización, enmascaramiento o generación de ruido, entre otras, se encuentren en el centro de la atención de muchas empresas y que se incorporen al ciclo de vida del dato en los sistemas de gobernanza de la información para garantizar el cumplimiento del RGPD y, por ende, proteger los derechos de los interesados.

No son sólo una medida de seguridad eficaz en la gestión de la privacidad sino también, especialmente las técnicas de anonimización y seudonimización, la puerta a proyectos de *data sharing* y *open data*.

Frente a estas dificultades, una vez más, el avance de la tecnología y la dinámica de mercado, algunos de los *boosters* más potentes para la innovación están replanteando los modelos de negocios tradicionales y generando nuevos modelos que llevan aparejados una visión distinta de la gestión y compartición de la información, como es el caso de los vehículos autónomos, donde distintos silos de datos y responsables de tratamiento buscan la forma de relacionarse entre sí de forma distinta a la tradicional.



**Data products are similar to consumer products in many ways.**

**Examples of similarities**

| | **Digital product** *Example: Computer app* | **Physical product** *Example: Car* | **Data product** |
|---|---|---|---|
| **Product features** | | | |
| **Customization of base product for different users** | App enables users to personalize the layout, color schemes, and content displayed and to select plans and pricing structures that meet their needs | Car buyers may purchase a variety of special options (eg, leather upholstery, tinted windows, antitheft systems) | Data products can be wired to support different systems that consume data, such as advanced analytics or reporting systems |
| **Delivery of regular product enhancements** | Automatic downloads of new functionality | New models<br><br>Engine modifications that boost fuel economy | New data<br><br>Support for additional consumption archetypes |
| **Production efficiency** | | | |
| **Reuse of existing processes, machinery, and components** | Software developers reuse blocks of code | Automakers use a common chassis on vastly different cars | Organizations reuse blueprints and modular technologies for consumption archetypes across products |

Fuente: McKinsey

Otra de las cuestiones que a menudo se debate entre los agentes del sector de la privacidad es la rigidez del sistema legal europeo frente, por ejemplo, al americano, mucho más orientado a la innovación. Y ello a pesar de que el propio RGPD indica que no es su intención convertirse en un obstáculo al tratamiento de datos personales sino crear un espacio de seguridad que favorezca su circulación y el progreso económico del espacio europeo.

Las razones de fondo de la disparidad de sistemas son diversas. Mientras el sistema norteamericano está más orientado a la economía y otorga mayor prioridad a la seguridad nacional, el sistema europeo está más orientado a los derechos sociales y concede prioridad a la garantía de estos derechos. También hay razones de carácter cultural implicadas y que el concepto de intimidad, subjetivo de por sí, no es concebido de la misma forma por ambos sistemas.

Pero no sólo aparecen diferencias cuando hablamos de marcos regulatorios extracomunitarios. Otra de las cuestiones que se puso de manifiesto en el marco de los trabajos que originan el presente informe es cierta disparidad en las interpretaciones que sobre determinadas cuestiones pueden encontrarse en las decisiones de las distintas autoridades de control europeas y las dificultades que estas suponen para el mercado y la innovación. En este sentido, y de cara a no convertir el RGPD por la vía de la aplicación en una nueva Directiva, el fomento de las herramientas y mecanismos de cooperación transfronteriza que prevé la normativa europea se atisba como un factor de mejora.

**Principios éticos en la gobernanza del dato**

Ligado al tema de la monetización, surge en el marco del debate sobre gobernanza de los datos y privacidad la cuestión de la ética en el uso de la información. Probablemente, a la sombra de grandes escándalos y sanciones, y por la presencia de tecnologías cuya injerencia en la privacidad resulta mayor (inteligencia artificial, tecnología biométrica, etc.) parece que los términos "explotación" y "monetización" de la información han adquirido cierta connotación negativa. Sin embargo, y como se ha mencionado con anterioridad, uno de los objetivos principales del RGPD es crear la seguridad jurídica necesaria para que el tratamiento de la información pueda, con el debido respeto a los derechos fundamentales, contribuir "al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas". Por tanto, es preciso luchar contra la negativización de la explotación de la información fomentando, entre sus principios, la ética, de tal forma que el beneficio resultante no sea únicamente económico, sino que contribuya al bienestar y beneficio social[3].

Incluir principios éticos en un sistema de *data governance* es, por ende, fundamental para garantizar el uso responsable, transparente y ético de los datos en una organización. En consecuencia, cada vez son más las empresas que identifican y defienden los principios éticos que quieren promover y trabajan por integrarlos en la gestión de la gestión de la información.

Para ello, es necesario que estos principios queden debidamente reflejados en las políticas y procedimientos que forman parte del sistema, incorporando directrices claras acerca de cómo tratar los datos con la debida transparencia y respeto al derecho de sus titulares, qué técnicas de recopilación y análisis son las más adecuadas de acuerdo con estos principios y, sobre todo, entendiendo cómo impacta a los titulares de la información el uso que se hace de ella.

Incorporar un perfil al equipo de gestión, asignar esta labor a alguno de los miembros del sistema de *data governance*, probablemente al *Chief Data Officer* o, incluso, crear un Comité de Ética que asuma esta labor, es una medida que contribuirá a la implantación y respeto de estos principios, como lo es también el recurso a las medidas formativas y de concienciación sobre la privacidad en la organización.

Asimismo, la puesta a disposición de los empleados de canales oportunos para reportar dudas o violaciones, y el establecimiento de sistemas de seguimiento y control, serán de utilidad a estos fines.

[3] Considerando 4. RGPD. "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad."

**Roles relacionados con la privacidad**

En un sistema de *data governance*, la responsabilidad de la privacidad de los datos se asigna principalmente a la figura del *Chief Privacy Officer* (CPO), que resulta la encargada de que el sistema cumpla con los principios y obligaciones en materia de protección de datos, así como de establecer políticas y prácticas relacionadas con la privacidad dentro de la organización.

No obstante, y a pesar de que ya se han cumplido cinco años desde la entrada en vigor del RGPD, lo que presupone ya cierta madurez en lo relativo a su aplicación, surge de forma recurrente la cuestión sobre la correcta identificación de los roles que en materia de privacidad pueden (o deben) aparecer en una empresa.

Son aún muchas las organizaciones que, por distintos motivos, no realizan la identificación de estos roles de acuerdo con lo establecido en el RGPD -de ahí que encontremos *Data Protection Officers* (DPO) desempeñando en realidad labores de *Chief Privacy Officers* y viceversa- o, simplemente, no cuentan con ellos.

Las principales razones de ello son la falta de recursos y la falta de concienciación sobre su relevancia. No todas las empresas pueden soportar el coste de estos roles, especialmente si son varios los que se requieren. Y es que, aún hoy, sigue siendo complicado para muchas empresas distinguir correctamente entre la función del DPO y el CPO.

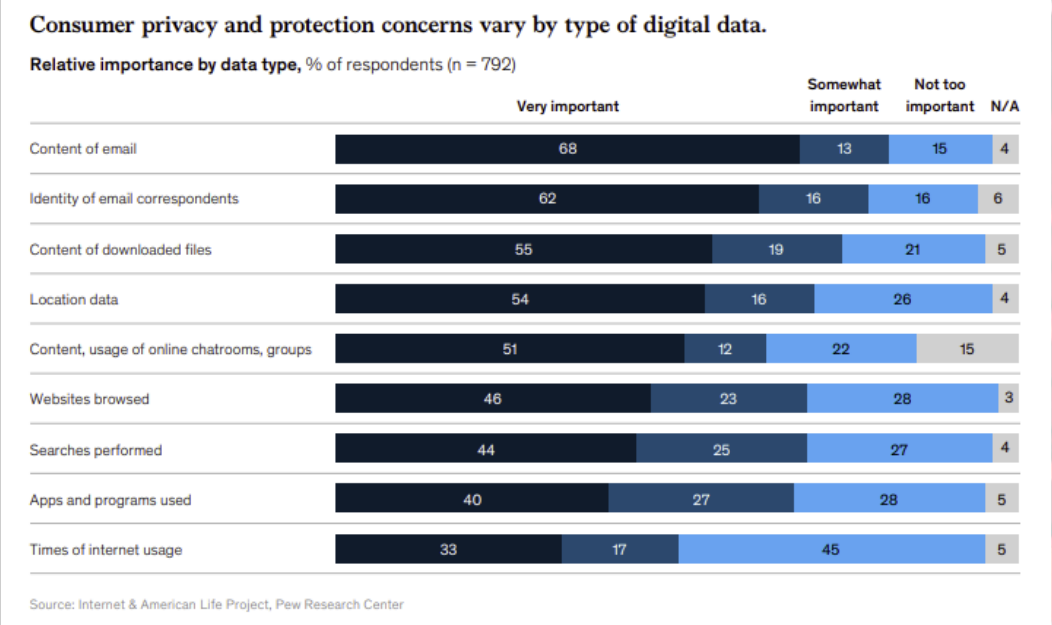
La figura del DPO, cuyos orígenes se remontan a la Ley Federal de Protección de Datos alemana de 1977 ha tenido siempre un papel supervisor en relación con el cumplimiento de la normativa de protección de datos y el RGPD lo rescata y dota de unas características (independencia, cualificación y posición en la empresa) y unas funciones específicas. Por su parte, el rol del *Chief Privacy Officer* tiene una visión más amplia de la privacidad en la organización que incluye aspectos éticos, estratégicos y operativos. Este último es, por tanto, el rol principal en materia de privacidad en el marco del sistema de gobernanza de la información.

En consonancia, con la mención a la supuesta madurez (o falta de ella) del ecosistema empresarial de cumplimiento del RGPD a la que se hacía mención, detecta el sector la necesidad de una mayor y mejor concienciación en relación con el impacto de la privacidad en cualquier empresa y la necesidad de dotarla no sólo de los roles necesarios, sino de los recursos suficientes para ello.

Aún se encuentra demasiado extendido el cumplimiento de carácter superficial sustentado, muchas veces, sobre la base del miedo a la sanción de la Autoridad de Control correspondiente y el cumplimiento de naturaleza reactiva (esto es, el provocado por la apertura de un expediente sancionador o tras las consecuencias de una brecha de seguridad).
El sector demanda una mayor concienciación sobre la necesidad de crear y dimensionar adecuadamente las estructuras necesarias para asegurar el cumplimiento de la normativa de privacidad, pero, sobre todo, sobre la relevancia e impacto positivo que esto genera sobre cualquier empresa.

Medidas como las contenidas en la Directiva (UE) 2016/1148 de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como NIS 2, aunque dirigida al ámbito de la ciberseguridad que de la privacidad, parece que pueden contribuir a la implicación de los puestos directivos de la organización por cuanto prevé sanciones especialmente dirigidas a ellos en determinados supuestos de incumplimiento.

La creciente preocupación de los consumidores por su privacidad y el incremento de las reclamaciones[4] que interponen ante las autoridades de control es, sin duda, otro de los factores que puede contribuir a mejorar el nivel de concienciación del sector empresarial.




Fuente: McKinsey

[4] Según la Memoria 2022 de la Agencia Española de Protección de Datos, existen una tendencia en aumento en el número de reclamaciones "con un aumento del 9% respecto al año 2021 y un 47% respecto del año 2020·.

**Tendencia creciente a entornos de seguridad delegada**

Cuando, en el contexto de una conversación sobre gobernanza del dato, el tema se centra en las infraestructuras y sistemas de información necesarios para hacerla posible, algunas de las cuestiones ineludibles son la tendencia a recurrir a proveedores externos, aumentando así el recurso a lo que se conoce como entornos de seguridad delegada, y la preocupación por la seguridad de estos entornos, habida cuenta del aumento constante de las brechas de seguridad.

Los entornos de seguridad de la información delegados son aquellos en los que una empresa confía en un proveedor externo, como un proveedor de servicios de seguridad gestionada (*Managed Security Service Provider* o Proveedor de Servicios Gestionados de Seguridad o MSSP,) o un proveedor de servicios en la nube, para gestionar y/o mantener la seguridad de su información y sistemas.

El aumento constante a este tipo de proveedores se basa en múltiples razones; entre ellas:

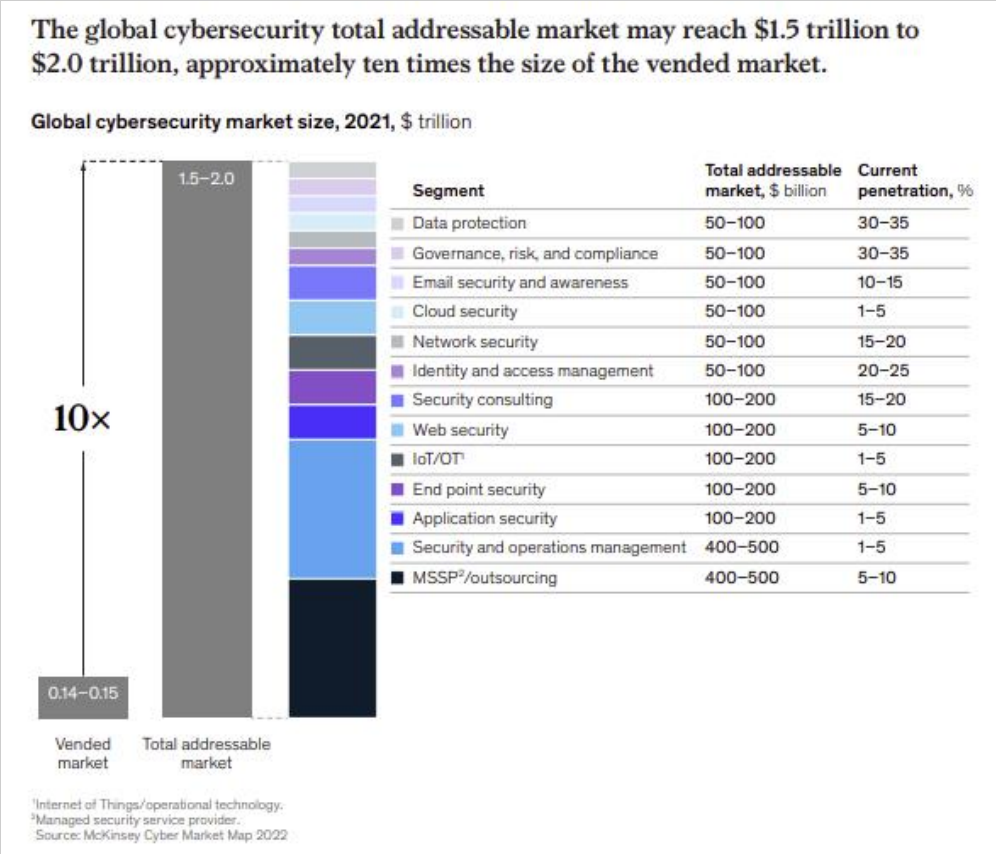
- Principalmente, la reducción de la inversión en la infraestructura de gestión y seguridad de la información. Contratar este tipo de servicios a un tercero suele ser significativamente más económico para una empresa que desarrollarlo por sí misma y se ofrecen sobre modelos de pago por uso o suscripción que resultan más asequibles.

- Contar con un proveedor externo permite a la empresa beneficiarse de su experiencia y conocimiento cualificado en el diseño, implementación y gestión de soluciones de seguridad, así como en la detección y respuesta a incidentes de seguridad. Además, la mayoría de los proveedores cuentan ya con certificaciones que permiten a la empresa no sólo ahorrarse el coste de su adquisición sino acreditar frente a terceros la solidez de sus sistemas.

- La flexibilidad que ofrecen los MSSP para adaptar y customizar sus productos a las necesidades específicas del cliente es, sin duda, otro de sus valores añadidos. Asimismo, están en constante proceso de mejora, liberando al cliente de esta labor.

- La experiencia en la prestación de estos servicios y los recursos con los que cuentan conceden a estos prestadores una eficacia mayor en la identificación de amenazas a la seguridad y en la respuesta ante cualquier incidente.

Contar con los servicios de un proveedor externo puede, por tanto, dotar a la empresa de sistemas especializados, maduros y en constante mejora.



**The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.**

**Global cybersecurity market size, 2021,** $ trillion



| Segment | Total addressable market, $ billion | Current penetration, % |
|---|---|---|
| Data protection | 50–100 | 30–35 |
| Governance, risk, and compliance | 50–100 | 30–35 |
| Email security and awareness | 50–100 | 10–15 |
| Cloud security | 50–100 | 1–5 |
| Network security | 50–100 | 15–20 |
| Identity and access management | 50–100 | 20–25 |
| Security consulting | 100–200 | 15–20 |
| Web security | 100–200 | 5–10 |
| IoT/OT[1] | 100–200 | 1–5 |
| End point security | 100–200 | 5–10 |
| Application security | 100–200 | 1–5 |
| Security and operations management | 400–500 | 1–5 |
| MSSP[2]/outsourcing | 400–500 | 5–10 |

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

Fuente: McKinsey

Ahora bien, es una obligación legal de la empresa, como responsable o encargada del tratamiento, seleccionar proveedores de servicios que ofrezcan garantías suficientes, por lo que una de las cuestiones que más preocupa en este momento al sector empresarial es el despliegue de la diligencia debida en su relación con estos terceros.

A tal fin las empresas no solo se encuentran con la necesidad de desplegar medidas de comprobación y diligencia en el momento de su selección, sino que deben diseñar procedimientos específicos que permitan mantener esta diligencia durante toda su relación con el proveedor, medidas que deben adecuarse a cada tipo de proveedor y a las características concretas del tratamiento de datos que realiza.

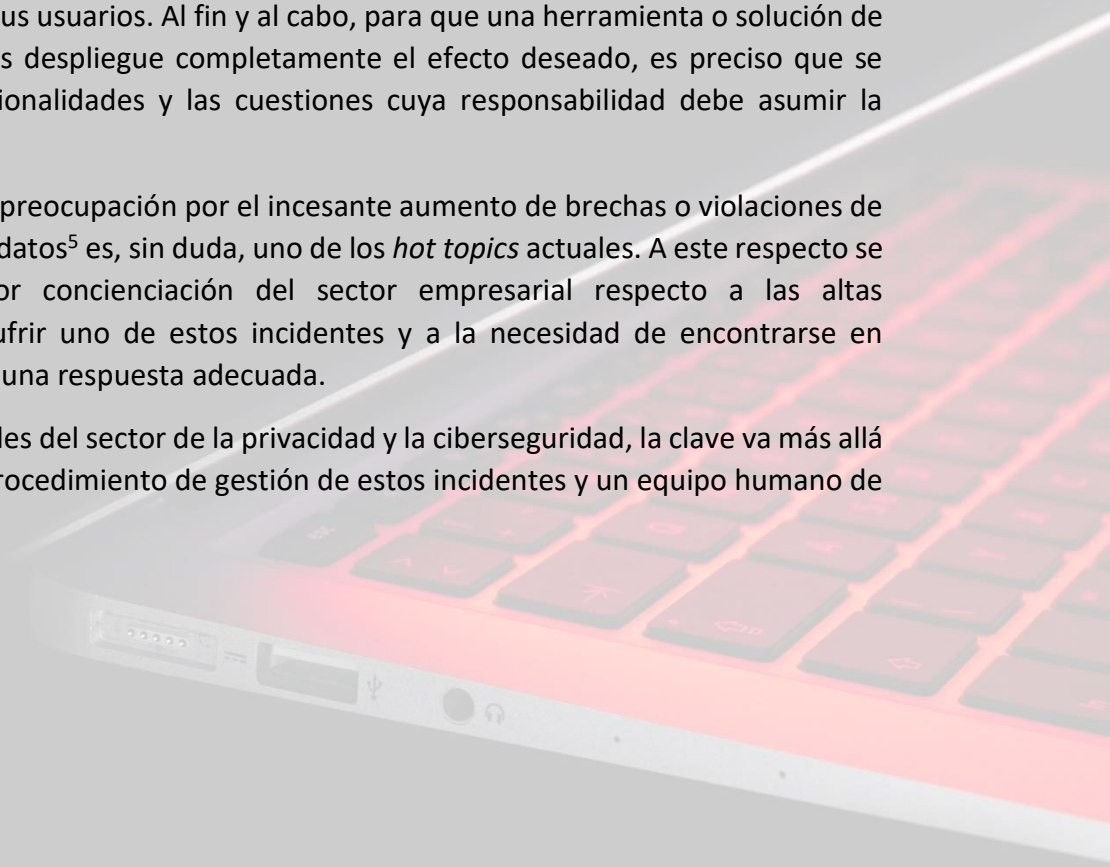
Otra de las dificultades identificadas en este sentido viene impuesta por la diversidad de marcos regulatorios que operan en relación con la privacidad y la seguridad de la información, especialmente en sectores regulados. Por ello, la tendencia es a la unificación de controles que simplifiquen en lo posible la labor de los equipos legales de las empresas.

Por otro lado, otra de las cuestiones que preocupan en relación con los MSSP, es la tendencia de ciertas empresas a considerar que, al contar con un proveedor externo, éste es quien se hará cargo del conjunto de obligaciones relacionadas con la seguridad de su información. Lejos de ser así, es preciso que la empresa supervise el servicio de forma regular mediante el diseño e implementación de los controles necesarios, el establecimiento de acuerdos de nivel de servicio claros en los contratos con los MSSP para garantizar que los estándares de seguridad se mantengan y se cumplan y asumiendo la responsabilidad de entender y cumplir con las responsabilidades en materia de medidas de seguridad que le corresponden.

Esta tendencia ha sido claramente detectada por los MSSP, de ahí que en los últimos tiempos sus soluciones cuenten con distintas herramientas de capacitación y concienciación de sus usuarios. Al fin y al cabo, para que una herramienta o solución de estas características despliegue completamente el efecto deseado, es preciso que se conozcan sus funcionalidades y las cuestiones cuya responsabilidad debe asumir la empresa.

Adicionalmente, la preocupación por el incesante aumento de brechas o violaciones de la seguridad de los datos[5] es, sin duda, uno de los *hot topics* actuales. A este respecto se percibe una mayor concienciación del sector empresarial respecto a las altas posibilidades de sufrir uno de estos incidentes y a la necesidad de encontrarse en condiciones de dar una respuesta adecuada.

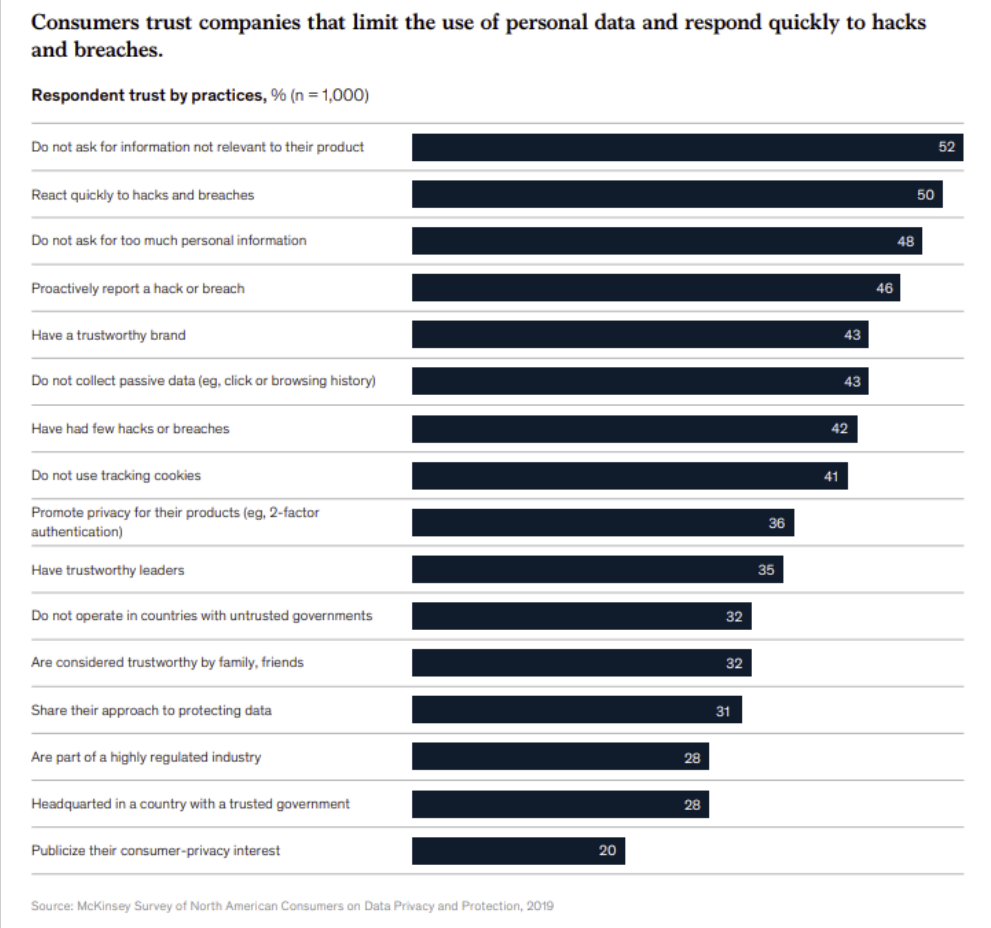
Para los profesionales del sector de la privacidad y la ciberseguridad, la clave va más allá de contar con un procedimiento de gestión de estos incidentes y un equipo humano de respuesta.



[5] Según el Instituto Nacional de Ciberseguridad (INCIBE) durante el 2022 ha participado en la gestión de más de 118.820 incidentes, lo que supone un 8,8 más que en 2021. Infografía_Balance de ciberseguridad 2022 (incibe.es)

Una brecha de seguridad es un momento de crisis en una organización, por lo que además de procedimientos o planes de contingencia que tengan en cuenta controles en materia de privacidad, seguridad y continuidad de negocio, equipo técnico y legal, se requiere:

- Un enfoque holístico del incidente que tenga en cuenta cuestiones de negocio y reputacionales.
- Preparación previa y ensayo a fin de que la urgencia y la sorpresa propia de entornos de crisis no repercuta en detrimento del éxito en la gestión del incidente.
- Diseño e implementación de medidas de seguimiento y medición de resultados a fin de convertir la fase de resiliencia propia de la gestión de este tipo de incidentes en un proceso de mejora continua.




Fuente: McKinsey

Por otro lado, llama la atención del sector empresarial la utilidad que las herramientas de Inteligencia Artificial (IA) parecen estar demostrando en la gestión de brechas de seguridad.

La IA puede resultar de utilidad en la identificación, detección y respuesta a las brechas de seguridad mejorando la velocidad y eficiencia. Así, la IA:

- Analiza con mayor agilidad grandes volúmenes de datos;
- Puede distinguir patrones de comportamiento de los usuarios sospechosos, por ser distintos de los habituales ya aprendidos;
- Es capaz contribuir a una detección más eficaz de actividades maliciosas e incidentes.
- Mejora la respuesta ante incidentes por la vía de la automatización;
- Puede mejorar el análisis forense digital posterior a las brechas de seguridad contribuyendo a la resiliencia de la organización.

Sin embargo, contar con herramientas dotas de IA no exime a las empresas de contar con personal altamente cualificado y con experiencia en ciberseguridad. De hecho, es la combinación de ambos factores lo que permitirá sacar el máximo partido de la herramienta y aplicar un enfoque prudente y diligente, habida cuenta de los retos asociados al uso de la IA (sesgos en los algoritmos, ética, etc.).

**Conclusiones**

La actual economía de los datos y el camino recorrido desde la entrada en vigor del RGPD, nos ha dotado de madurez en la gestión de la información y sobre todo objetivos a perseguir. No obstante, la realidad es que este grado de madurez es aún perfectible, de hecho, debe ser enfocado siempre en el marco de un proceso de mejora continua.

La implementación de sistemas de *data governance* o gobernanza del dato está demostrando ser una vía para la consecución de la referida madurez que permite a las empresas una gestión de la información ágil, flexible y segura, alineada con su estrategia comercial de tal forma que la organización pueda empezar a percibir estos sistemas y los recursos involucrados en ella como una inversión y una oportunidad.

Procedimientos, personas e infraestructura, son la clave en la construcción de estos sistemas. Asimismo y, como en cualquier proceso de cambio, se requiere un cambio cultural de la organización en el que los profesionales de la privacidad desempeñan un papel estratégico, si bien es cierto que se requiere mayor concienciación e involucración de los equipos directivos para llevar el cumplimiento en materia de protección de datos y seguridad al siguiente nivel de madurez.

# Agradecimientos:

*Han participado en el focus group de IA del Obervatorio IE – ECIJA de Derecho Digital los siguientes profesionales:*

- Marta Duelo, Chief Legal Officer en Mobile World Capital
- Marcos García-Gasco, Associate Legal Director (DPO Europe) en Xiaomi
- Ana Regidor, Chief Privacy Officer en Amadeus
- Borja Larrumbide, Security Assurance for Spain and Portugal en Amazon Web Services
- Mireia Martínez, Head of Legal, International & Data Privacy en Glovo
- Miguel Álvarez, Head of Legal and manager of the in-house Legal team en Canon
- Macarena Rosado, General Counsel en IE University

*En este informe, los participantes compartieron sus experiencias, conocimientos y opiniones sobre los sistemas de data governance. Estas opiniones son responsabilidad del autor y no necesariamente representan los de la empresa.*