Ejerciendo los derechos de acceso en España

Un estudio comparativo antes y después del RGPD

info@eticasfoundation.org | +34936005400

Eticas Foundation. Calle Mir Geribert, 8, 08014 Barcelona

Introducción

Este estudio describe las experiencias de intentar ejercer el derecho de acceso a los datos personales en España.

Usando diferentes ejemplos etnográficos, el estudio prueba cuán fácil o difícil es para un sujeto de datos con sede en España obtener sus datos personales, en primer lugar, **ubicando la información requerida sobre las organizaciones y sus controladores de datos** y, en segundo lugar, **enviando solicitudes de acceso** de personas a estas organizaciones.

La **primera parte del trabajo** de campo se realizó hace unos años, en **2014**, cuando Eticas participaba en un proyecto de investigación europeo más amplio, en el cual diferentes países europeos realizaban solicitudes de acceso para saber cómo los organismos públicos y privados cumplían (o no) con la ley.

La **segunda parte del trabajo** de campo se realizó en **2018** por parte del equipo de Eticas Foundation y colaboradores, para comprender mejor cómo se estaba aplicando el nuevo Reglamento General de Protección de Datos europeo (**RGPD**), en relación con el derecho de acceso a los datos personales.

El **derecho a la protección de datos personales** se deriva de los **artículos 10 y 18.4** de la **Constitución española** que salvaguardan la dignidad y la privacidad de las personas, respectivamente. Fue desarrollado en la **Ley Orgánica 367 15/1999 de Protección de Datos Personales** (Ley Orgánica de Protección de Datos, LOPD), que era la ley aplicable en España antes del **RGPD**. El Reglamento europeo general de protección de datos que entró en vigor en mayo de 2018 comportó una nueva ley española, que se aprobó en diciembre de 2018: la **Ley Orgánica 3/2018**, de 5 de diciembre, sobre protección de datos personales y garantía de derechos digitales.

Con **RGPD**, las **entidades responsables del tratamiento** de datos personales deben ofrecer a una **persona solicitante del derecho de acceso** la siguiente información:

(1) las **categorías de datos** personales que se tratan, (2) cuáles son las **finalidades del tratamiento,** (3) a qué **destinatarios** o categorías de destinatarios se comunicaron o se comunicarán estos datos, (4) información sobre el **origen de los datos** cuando el origen no ha sido la misma persona interesada, y (5) una **copia de los datos** personales objeto de tratamiento si la persona interesada así lo solicita. Además, (6) debe informar del **plazo previsto de conservación** de los datos y (7) de los **criterios** que se han seguido para determinar dichos plazos. Finalmente, debe informar (8) de que la persona interesada tiene también derecho a **solicitar la rectificación** o **supresión** de sus datos, la **limitación** del tratamiento, **oposición** al tratamiento, y también a **presentar una queja** ante la autoridad de control (agencia de protección de datos que corresponda por cada territorio).

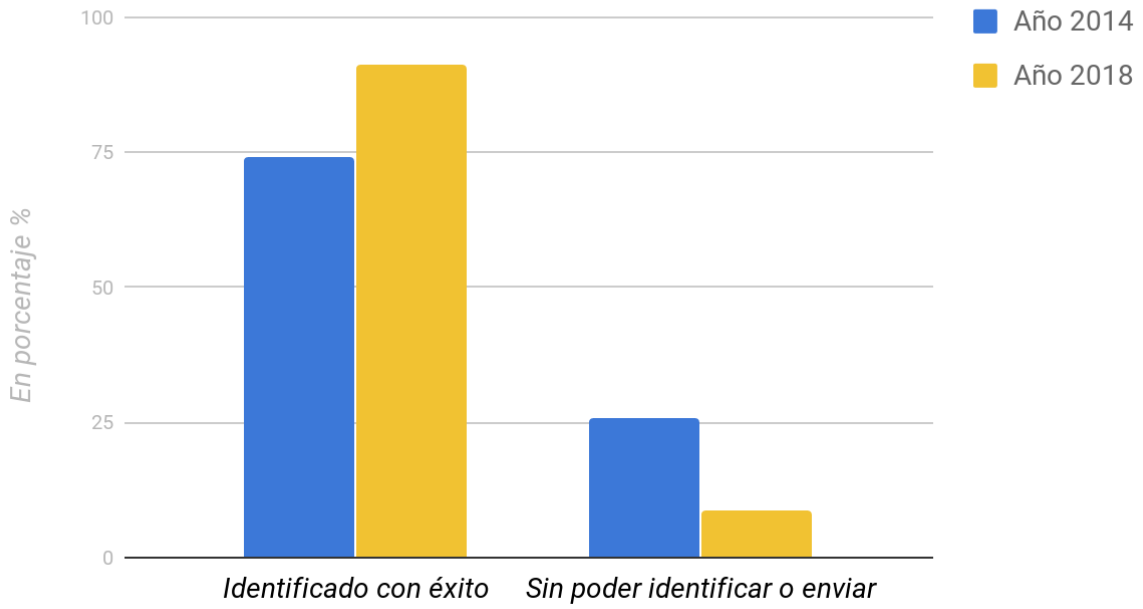
Derechos de acceso en España: año 2014

Esta parte describe, analiza y resume la experiencia acumulada durante nuestros **intentos de localizar controladores de datos** y, una vez hecho esto, **enviar solicitudes de acceso** a las organizaciones.

Como parte de este proceso, intentamos ubicar los controladores de datos en **30 organizaciones** y posteriormente enviar **21 solicitudes de acceso** de personas a una amplia gama de controladores de datos **tanto en el sector público como en el privado en España** y, en el caso de ciertas empresas multinacionales, más allá de sus fronteras.

Los detalles del controlador de datos se encontraban **habitualmente en los sitios web** oficiales de las organizaciones. En los casos en que los sitios web no resultaban útiles para ello, a menudo era **necesario ponerse en contacto** con las organizaciones **por teléfono**.

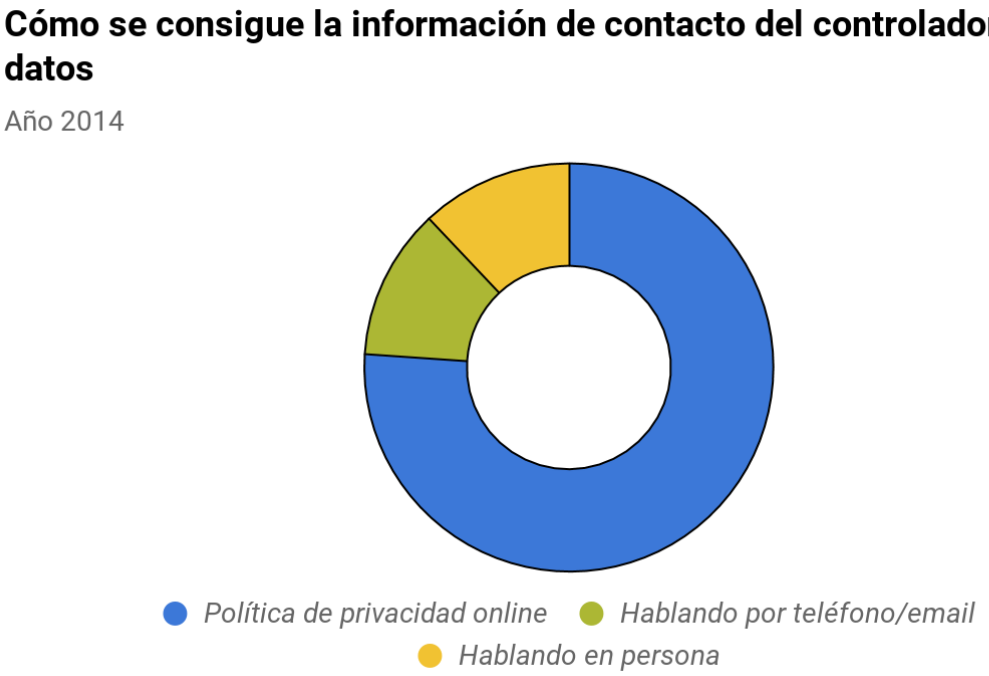
Localizar la información del controlador de datos



En el año **2014 pudimos identificar con éxito un 74% de los datos de contacto** de las organizaciones, y en **2018 pudimos obtener mejores resultado**s, identificando correctamente los detalles de contacto **en un 91,18% de los casos**. También dicho de otro modo, en 2014 no pudimos llegar a obtener la información para ejercer los derechos de acceso a nuestros datos en un 26% de los casos, mientras que en 2018 se trató "solamente" de un 8,82% de los casos donde no pudimos resolver el envío de nuestras solicitudes. Hay signos de mejora, pero aún detectamos algún nivel de incumplimiento.

Nuestra experiencia fue que cuando hablamos con los miembros del personal por teléfono, era evidente una **falta general de experiencia sobre la protección de datos y los derechos de acceso.** Estas conversaciones resultaron bastante difíciles debido a la **sospecha sistemática** de los encuestados, que parecían escépticos de que quisiéramos acceder a nuestros datos personales simplemente porque teníamos curiosidad.

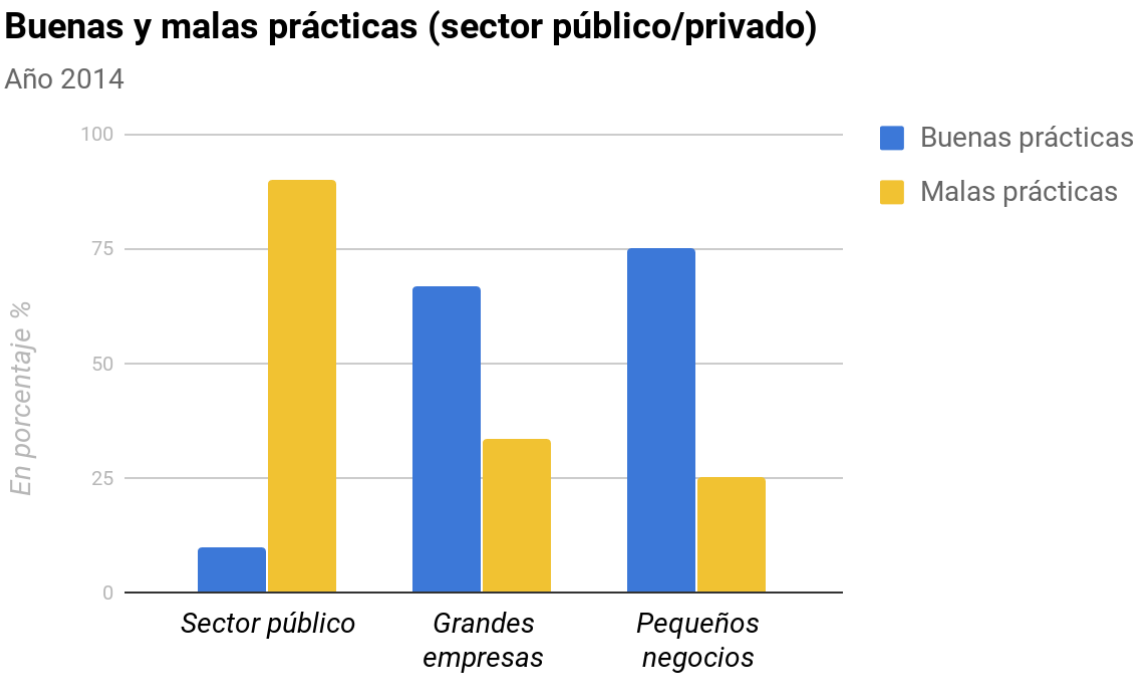
Los casos en los que **pudimos encontrar los datos de contacto a través de las políticas de privacidad de las páginas web** de las organizaciones fueron los que más, un total de **19 casos**, mientras que en **3 casos tuvimos que hablar por teléfono** con personal de estas entidades, o en otros **3 casos tuvimos que hablar en persona** dirigiéndonos físicamente hasta la sede de la organización.



En el caso de los **sistemas de CCTV**, la **señalización obligatoria** debería haber comportado que podríamos ubicar el controlador de datos sin hablar con ningún miembro del personal en persona. En el caso de los sitios de CCTV, **se encontraron irregularidades** en la señalización debido a una **ubicación deficiente e invisibilidad**, ninguna señalización, o señalización sin detalles del controlador de datos. **Solo en dos de cinco sitios se encontró una señalización con buen cumplimiento de la ley española**.

La solicitud de acceso a datos personales en España generalmente no es un proceso tan sencillo como quizás debería ser. En términos de prácticas facilitadoras / restrictivas, se pudieron observar diferentes tendencias. **En la mayoría de los casos en los que habíamos recibido respuestas, estas habían sido incompletas**.

Así, cuando hicimos este trabajo de campo (año 2014), **descubrimos que el grado general de cumplimiento legal y el desempeño de buenas prácticas cuando los ciudadanos intentaban ejercer sus derechos de acceso en España eran bajos**. Por Algunas organizaciones no respondieron a nuestras solicitudes en ningún momento y solo se consideró que una minoría de los casos dio lugar a respuestas legalmente adecuadas después de un proceso relativamente sencillo y directo.



Especialmente el **sector público** mostró un bajo nivel de cumplimiento, con un **90% de malas prácticas**, y sólo un 10% de buenas prácticas, mientras que el **sector privado** tenía un

cumplimiento siempre mucho más alto, de un **66,7% de buenas prácticas en grandes corporaciones** hasta un **75% de buenas prácticas en pequeños negocios**.

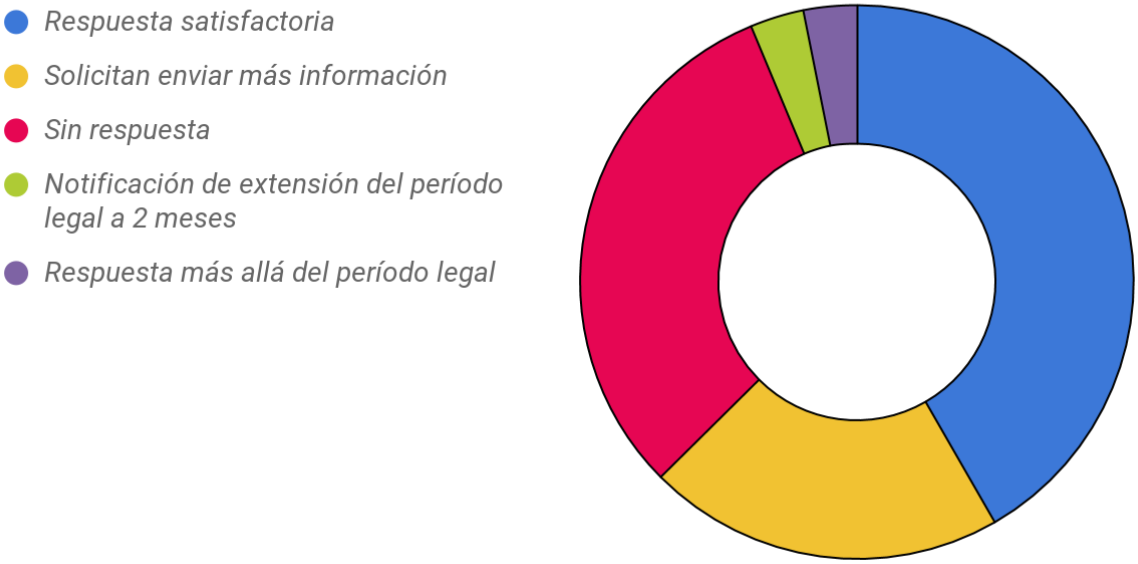
Vale la pena mencionar que nuestras **experiencias difirieron según el tipo de datos que solicitamos**. Si bien resultó mucho más fácil obtener la divulgación de datos personales, las preguntas sobre los procesos automatizados de toma de decisiones y el intercambio de datos con terceros permanecieron sin respuesta. Esto puede ser el resultado de una falla en el seguimiento de cómo se usan y comparten los datos, por lo que algunas organizaciones no estaban dispuestas a responder nuestras preguntas sobre esto.

Después de este estudio, **concluimos con una reflexión sobre cuán alejados estábamos de nuestros datos personales.** Algo que nos pertenece y algo sobre nosotros debe estar protegido por la ley. Cuando un ciudadano común, sin una razón en particular que no sea un deseo de aumentar su conocimiento informativo, presentaba solicitudes de acceso, a menudo comenzaba un viaje que le llevaba a tener que navegar por un laberinto y terminaba, no siempre felizmente, cuando había completado toda una pista de obstáculos.

En este sentido, **¿cómo sería la situación 4 años después, y con la nueva regulación europea sobre protección de datos ya en vigor?** Para responder a esa pregunta, decidimos volver a poner nuestros derechos de acceso en práctica.

Derechos de acceso en España (2018) bajo RGPD

En esta ocasión para realizar el trabajo de campo **buscamos el contacto de 34 controladores de datos**, de los que finalmente **pudimos efectuar 31 peticiones** de acceso a datos personales (91,18%), correspondientes tanto a empresas y organismos del sector público como del sector privado. Las **3 peticiones de acceso que no pudimos llegar a llevar a cabo** (8,82% de los casos) fueron, en dos de ellos, porque no fue posible localizar los datos de contacto para realizarla, y en otro caso, el formulario contenía un error y no dejaba introducir el código postal correspondiente, y por tanto no dejaba enviar la petición.

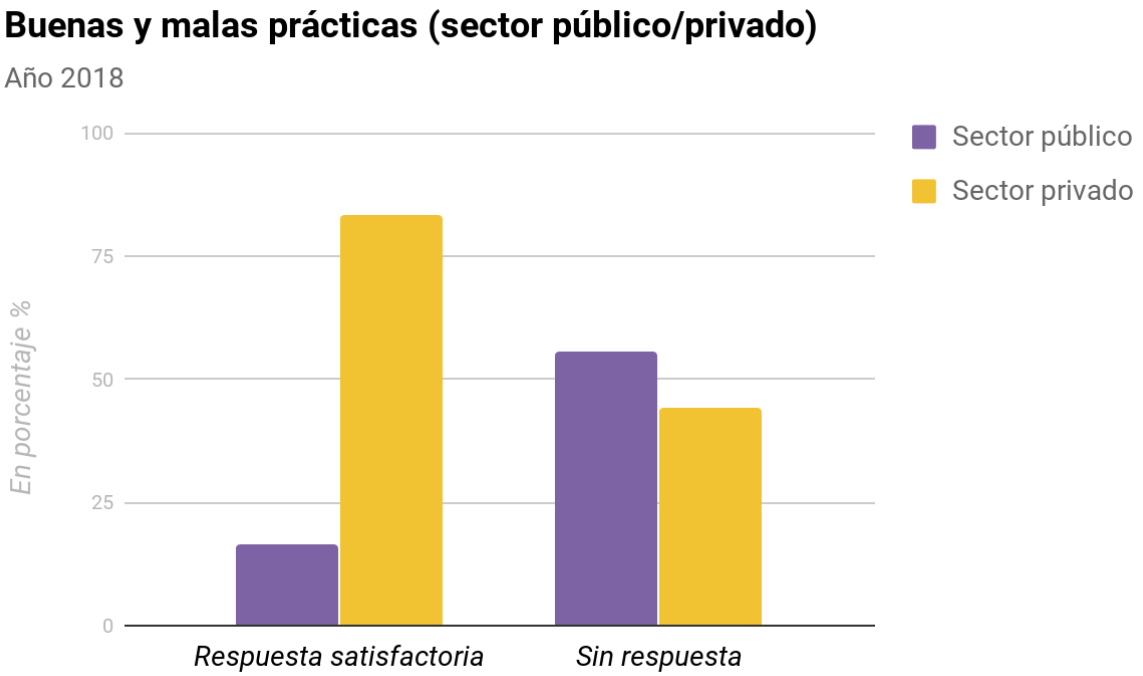


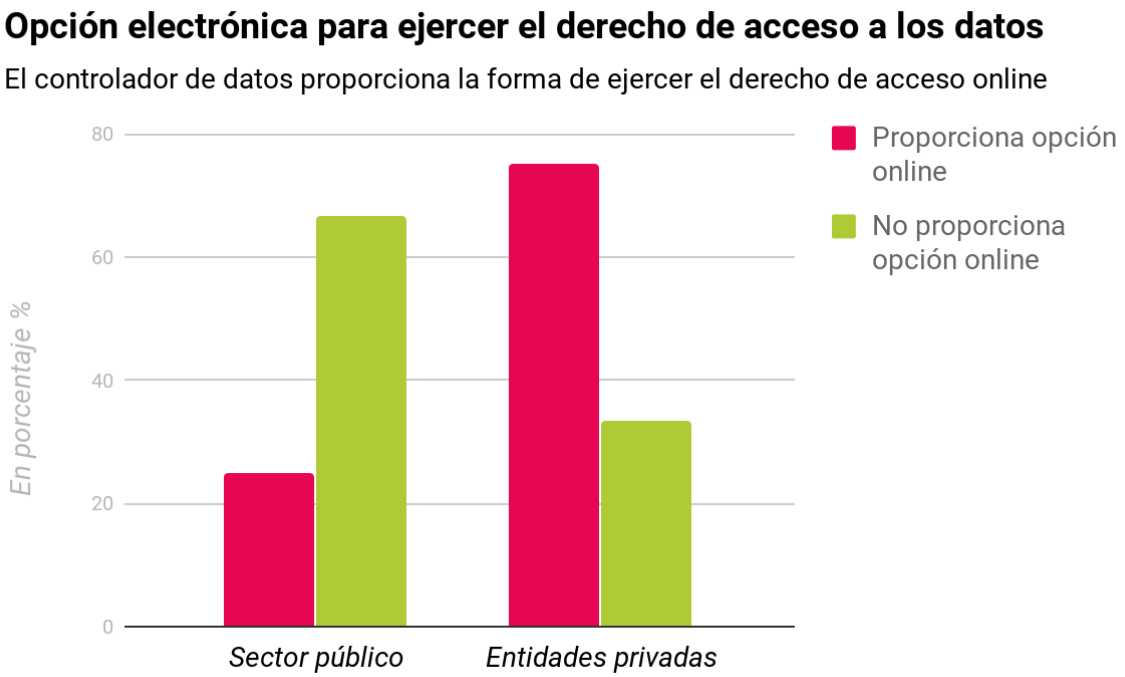
El **nivel de cumplimiento** fue bastante **desigual**. De las 31 peticiones de acceso que pudimos hacer, solamente **12 fueron respuestas de manera óptima y directa (38,71%)**, es decir, respuestas que ofrecían una información correcta dentro del plazo establecido. Por otro lado, **6 respuestas recibidas solicitaban algo más de información** de parte de la persona interesada **(19,35%)** para que la petición se pudiera seguir procesando: 2 pedían enviar una copia del documento de identidad; **1 efectuó incluso una llamada telefónica a la interesada** preguntándole de qué datos quería recibir información (**y por qué motivos**); y en 2 casos pedían las dos cosas, es decir, que proporcionáramos un documento de identidad y que especificáramos a qué información se deseaba acceder.

Sólo **en 1 caso** recibimos una respuesta que era una **comunicación de ampliación del plazo** legalmente establecido de 30 días a 2 meses para dar una respuesta, tal y como prevé RGPD, argumentando que se trataba de una petición compleja dada la gran cantidad de datos que gestiona el organismo.

Si 12 fueron respuestas directamente, y 7 fueron respuestas pero sin ofrecer en un primer momento los datos personales solicitados, **las peticiones enviadas de las que no obtuvimos ninguna respuesta fueron un total de 9, lo que es casi un 30% (29,03%).** Además, añadidos a estos, en 1 caso, **recibimos una respuesta fuera del plazo** que establece la ley.

Por sectores, **el sector privado en general responde mejor que el sector público**. La misma tendencia encontrada en el año 2014. Consideramos 34 controladores de datos, de los cuales 21 eran actores privados y 13 actores públicos. De las **respuestas más satisfactorias**, sólo un **16,67%** corresponde a **entidades del sector público**, y el resto (**83,3%**) son **empresas privadas**. Por el contrario, de los casos de los que no recibimos respuesta, un 55,6% de corresponde a entidades del sector público, y el 44,4% a entidades privadas.





En cuanto a la opción que recoge la nueva legislación europea relativa a proporcionar una vía electrónica mediante la cual ejercer el derecho de acceso (RGPD, considerando 59), en la LOPDGDD no se considera una obligación sino una opción más entre otras. Así, de las organizaciones incorporadas en el estudio, 20 **lo ofrecen** (**un 64,52% de entidades**), pero 12 **no**, es decir, **un 38,71%**. Y por sectores, **las que no son mayoritariamente del sector público**, un **66,67%**, frente a un **33,33%** de empresas del sector privado. En cuanto a las que sí cumplen con esta opción contemplada por la ley, 15 son empresas privadas y 5 públicas, con un 75% y un 25% respectivamente.

De los casos de acceso a datos que solicitamos, **vale la pena resaltar cuando recibimos una llamada al móvil** con preguntas sobre los motivos de por qué se quería llevar a cabo esta acción, que en definitiva no es sino ejercer un derecho: buscando qué información, si lo hacíamos por razones profesionales o privadas, si es que había habido algún problema con la entidad en concreto, etc. Experimentamos así el rastro de **una desconfianza y unas suspicacias** que aún permanecían, como las que habíamos experimentado en la oleada de peticiones anterior de 2014. En otro caso, incluso nos pedían ir personalmente para identificarse. O también, el caso en

que recibimos un correo electrónico que prácticamente no se podía leer, un texto sin formato, con código html y utilizando una jerga legal.

Conclusión

Hemos mejorado algo, sí: en **acceder a los datos de contacto donde poder ejercer los derechos de acceso**, pasando **de un 74% de éxito en 2014 a un 91,18% en 2018**. Y también hemos mejorado en **poder acceder a estos datos de contacto mediante consulta online** (sin tener que visitar el organismo personalmente ni tener que llamar por teléfono), pero todavía vemos un nivel bastante bajo de ofrecimiento del derecho de acceso por medios electrónicos, ya que casi un 40% no lo proporcionan (38,71%).

Y todavía quedan prácticas poco afines a la protección de datos como la que relatamos de la llamada telefónica, aunque en este caso debido a que la interacción personal es menor hemos encontrado solamente uno.

Finalmente, el **sector público sigue estando por detrás del sector privado en buenas prácticas, pero va mejorando**, pues ostentaba el 90% de las malas prácticas en 2014, y el 2018 representa un 55,6% de las entidades que no ofrecen ninguna respuesta. También siguen yendo por detrás, como veíamos en los porcentajes, ofreciendo una vía electrónica para ejercer el derecho de acceso, respecto a entes privados.

Casos de estudio - año 2014

Sector público

Control de fronteras – Schengen Information System
Solicitar acceso a datos personales fue fructífero y sencillo en este caso. Por lo tanto, el procedimiento fue relativamente simple y directo, y puede considerarse como una muestra de buenas prácticas.
Antecedentes policiales - Ministerio del Interior, Dirección General de la Policía
Tres días después de que enviamos nuestra carta, el controlador de datos envió una notificación informándonos que nuestra solicitud estaba siendo procesada. Un mes después, (un poco más allá del límite de tiempo legal para realizar las respuestas), su respuesta concluyó que no había información en sus archivos sobre el solicitante. La carta iba firmada por un oficial de alto rango dentro del departamento, con un tono formal y neutral.
Registro de licencias de conducción
Esta agencia pública demostró un mal cumplimiento en términos de obtener una respuesta satisfactoria a nuestra solicitud. Después de tres intentos de obtener la información deseada, nos quedamos con pocas opciones, excepto presentar una queja oficial ante la APD nacional. Posteriormente, recibimos una respuesta de la APD en la que indicaron que nuestros derechos de acceso habían sido satisfechos. Sin embargo, no estuvimos de acuerdo, ya que una de nuestras preguntas había sido ignorada.
Europol
Presentamos nuestra solicitud de datos sobre nosotros en las bases de datos de Europol a través de la Policía. Su carta se basó en una exención legal que permite a las fuerzas de seguridad denegar el acceso a los ciudadanos. En general, encontramos que este caso mostraba prácticas restrictivas. El uso de jerga legal compleja parecía ser usado como un escudo para desalentar a los ciudadanos a enviar consultas de seguimiento.
Servei Català de Trànsit (Servicio Catalán de Tráfico)
Nuestra primera solicitud de llamada telefónica quedó sin respuesta. Enviamos una segunda carta agregando que presentaríamos una queja oficial a la APD española si no se recibía una respuesta. Esta segunda carta fue respondida más allá del límite de tiempo legal y con información incorrecta. Hicimos una queja oficial a la DPA

española que se remitió a la APDCAT (la APD catalana). Cinco meses después, la DPA catalana dictaminó que la organización debería revisar nuestra solicitud y revelar nuestros datos personales, cosa que hicieron.

Sector privado

Operador de telefonía móvil
La información encontrada en el sitio web oficial fue clara y directa. El controlador de datos nos respondió dentro del límite de tiempo legal. La carta explicaba que no practican los procesos automáticos de toma de decisiones, y que el intercambio de datos se limita a las acciones necesarias para el cumplimiento de los servicios ofrecidos por la organización. La carta iba firmada pero sin dar ningún nombre o departamento específico.
Tarjeta de fidelidad (supermercado)
Encontramos rápidamente en el sitio web de la compañía la información sobre cómo ejercer los derechos de acceso. Presentamos nuestra solicitud y recibimos una respuesta en el plazo de un par de semanas. En resumen, pudimos ejercer nuestros derechos con poca dificultad y se puede decir que la organización empleó prácticas abiertas y de facilitación.
Tarjeta de fidelidad (tienda de comida)
La organización respondió dentro del plazo legal, alegando que no tenían datos disponibles sobre el solicitante, a pesar de que el investigador tenía la tarjeta (fidelización de clientes) del "club de fans". En una segunda carta, la compañía explicó que la razón por la que no tenían datos sobre nosotros era porque los datos del club de tarjetas de fidelidad son anónimos. Consideramos este caso como un ejemplo de buena práctica.
Amazon
Dos días después de hablar con alguien por teléfono, recibimos información sobre su política de privacidad y contraseñas que debían desbloquear un CD-ROM. La respuesta fue incompleta y no pudimos desbloquear el CD-ROM. Casi dos meses después de nuestra primera solicitud, finalmente recibimos las contraseñas correctas. Contenía información valiosa, como una lista de destinatarios con los que se comparten los datos. Este fue un gran ejemplo de una política de facilitación socavada por prácticas ineficientes y un mal mantenimiento en el tiempo.

Registros bancarios
La información sobre cómo ejercer los derechos de acceso se encontró fácilmente en el sitio web oficial de la organización. Después de enviar dos solicitudes sin respuesta, presentamos una queja oficial a través de la APD española. Durante el proceso de resolución de disputas, el banco no se comunicó con la APD a pesar de tener la oportunidad de proporcionar argumentos en contra. Por lo tanto, la APD encontró que el banco había actuado incorrectamente a través de prácticas administrativas deficientes.
Facebook
El sitio web sólo ofrecía cómo descargar datos personales. Como no queríamos hacer esto sino enviar una solicitud a la empresa, enviamos una carta a su sede europea en Irlanda. Varias semanas después, asumimos que nuestra solicitud no se había entregado, ya que no habíamos recibido una respuesta de Facebook o el acuse de recibo de la oficina postal. Enviamos una segunda carta diciendo que presentaríamos una queja a la APD si no se recibía respuesta a partir de entonces. Facebook no respondió, por lo que presentamos una queja oficial a la APD española. Aunque habíamos enviado nuestra solicitud a Facebook en Irlanda, la APD española atendió nuestra queja y se puso en contaco con Facebook. Después de considerar nuestra queja, y esperando la respuesta de Facebook, la APD nos informó que estarían a nuestro favor.
Google
Google fue otro ejemplo de prácticas extremadamente malas en términos de ubicación de controladores de datos y protección de datos. Respondieron más allá del límite de tiempo legal y su respuesta puede considerarse incompleta. Al final, hicimos una queja oficial a través de la APD española. Algunas semanas después, recibimos una respuesta de la APD que decía que nuestra queja no sería confirmada. Esto se atribuyó a la falta de información en nuestra queja original. Esto parece que era algo inusual, ya que nuestra queja era similar a otras quejas (confirmadas) que se presentaron como parte de esta investigación.
Sistema de datos "Advanced Passenger Information"
Esta solicitud tuvo que ser enviada a los Países Bajos (con un cargo postal adicional). Un mes después (un poco más allá de los límites legales), recibimos una segunda respuesta algo corta e incompleta. Respondimos pidiendo más información pero no recibimos respuesta. Como resultado, presentamos una queja ante la APD española, que nos dijo que escribiéramos a la APD holandesa directamente.
Microsoft El contenido online proporcionado por Microsoft era algo complicado. Aunque su política de privacidad fue fácil de localizar, no proporcionaba la vía para realizar una solicitud de acceso. No recibimos respuesta a nuestra primera solicitud, por lo que hicimos un segundo intento. Esta vez, recibimos un correo electrónico genérico que no consideró nuestra consulta correctamente. Respondimos y pedimos más información, pero una vez más no

hubo respuesta. Hicimos una queja oficial ante la APD española, que luego decidió no defender nuestra queja ya que aparentemente no habíamos proporcionado información suficiente.
Twitter
La página web oficial de Twitter ofrecía información clara, a través de su política de privacidad, sobre qué datos recopilaban y con qué fines. Enviamos nuestra primera solicitud por correo, pero no obtuvimos respuesta después del período de 30 días, por lo que enviamos una segunda solicitud por correo electrónico. Nos dieron un número de caso, pero no recibimos ninguna respuesta posterior y, por lo tanto, procedimos a presentar una queja ante la APD española. La APD española nos dijo que contactáramos con la APD estadounidense. Al final, ni Twitter ni la APD española parecían inclinados a resolver este asunto mediante el uso de prácticas facilitadoras transparentes. En cambio, la carga cayó sobre el solicitante.
CCTV (Circuito cerrado de televisión) en un estadio
Hay dos controladores de datos en un estadio: el club de fútbol y la policía local. Presentamos nuestra primera solicitud a la Policía. Nos pidieron que proporcionáramos más información, por lo que enviamos la documentación solicitada y respondieron diciendo que debíamos enviar los documentos al club de fútbol. Esto puede ser considerado una práctica disuasiva. Luego contactamos al club de fútbol por carta y no recibimos respuesta, por lo que nos contactamos nuevamente con la organización por correo electrónico. El club respondió diciendo que no habían recibido la solicitud original (lo que contradice el recibo de entrega que obtuvimos de la oficina de correos). Después de algunos intentos más, presentamos una queja oficial a la APD con respecto a ambos controladores de datos.
CCTV en un espacio público / centro de la ciudad
No pudimos localizar ninguna señalización una vez visitado el lugar en persona, pero pudimos identificar a la organización responsable como el Ayuntamiento y presentar nuestra solicitud. Varias semanas después de nuestra solicitud, volvimos a visitar el sitio y encontramos varias señales nuevas que brindaban información sobre los controladores de datos. Luego recibimos una respuesta del ayuntamiento. Su respuesta fue una sola hoja de papel que nos fue entregada personalmente en casa por un mensajero. La falta de un sobre demostraba cómo solicitar información puede llevar a la divulgación de datos personales adicionales. Nos negaron el acceso a las imágenes, así que lo solicitamos nuevamente y recibimos otra negativa. La APD regional no confirmó nuestra queja basando su respuesta en el borrado de las imágenes y la imposibilidad de acceder a nuestros datos registrados.
CCTV en el transporte público
La señalización en el lugar identificaba adecuadamente el controlador de datos. Enviamos una solicitud a esta organización y respondieron dentro del límite legal de tiempo, pero el mensaje no fue de ayuda y mostró

hostilidad. El recibo de entrega obtenido en la oficina de correos mostraba que el controlador de datos tuvo la oportunidad de guardar estos datos, pero no lo hizo. Después de otros dos intentos fallidos, presentamos una queja a la APD española. Unos días más tarde, recibimos una respuesta de la oficina de servicio al cliente, donde identificaron al solicitante en las imágenes de CCTV. Simplemente describieron lo que aparece en sus grabaciones (esto cumple con la ley). En resumen, actuaron como si nuestra solicitud hubiera sido inútil y llevara mucho tiempo para ellos.
CCTV en un gran supermercado
Aunque la señalización de CCTV era fácil de ubicar y proporcionaba los datos de contacto del controlador de datos, esta organización generalmente mostró prácticas deficientes. Hubo confusión administrativa cuando la organización recibió nuestra carta. Por lo tanto, su razón para eliminar el material de archivo se basó en un marco de tiempo inexacto. Vimos esto como una estrategia de negación. Dado que consideramos que utilizaban prácticas restrictivas, presentamos una queja oficial a través de la APD española. La APD no confirmó nuestra decisión y dijo que la tienda departamental había proporcionado la respuesta legalmente requerida (es decir, que no se puede ver la grabación porque ya se ha borrado). Sin embargo, nos decepcionó que la APD no reconociera que habíamos enviado la solicitud dos veces. En nuestra segunda solicitud, habíamos sido especialmente cuidadosos con el tiempo para evitar exactamente esta excusa.
CCTV en un banco
La señalización en la puerta era claramente visible, pero la identificación del operador de CCTV y los datos de contacto no eran muy legibles. Presentamos nuestra solicitud al banco por escrito y respondieron explicando que habían rechazado nuestra solicitud por una variedad de disposiciones legales que establecen que el CCTV capturado en lugares financieros solo puede ser divulgado a las fuerzas de seguridad. Preguntamos a la APD si esta era una lectura correcta de la ley y la APD respondió acorde con la interpretación del banco, de su no obligación de divulgar las imágenes.
CCTV en un edificio del gobierno
La señalización mostrada en este lugar estaba en total cumplimiento con la ley. Era visible, se encontraba en cada entrada del edificio y proporcionaba información de contacto. Presentamos nuestra solicitud por escrito y recibimos una respuesta unas semanas después. La carta no resultó útil, así que hicimos una queja oficial a través de la APD española. La denuncia fue trasladada a la Agencia Catalana de Protección de Datos. Al final, nuestra queja fue rechazada porque la APD encontró que en nuestra solicitud, deberíamos haber especificado exactamente qué bases de datos / archivos deseábamos que buscaran. La decisión de la APD fue destacable, ya que parecía exigir que supiéramos, antes de realizar una solicitud, dónde se pueden ubicar nuestros datos personales y, por lo tanto, excluir las solicitudes generales para saber si una organización procesa algún tipo de información sobre uno mismo.

Casos de estudio - año 2018

Sector público

Cat Salut
Envío de carta portal sin ninguna respuesta. Sí en cambio que llega una respuesta del CAP Drassanes, también gestionado por Cat Salut (caso que explicamos a continuación).
CAP Drassanes
La persona que hace la petición recibe una llamada en su teléfono móvil, y la interlocutora se identifica como miembro del equipo responsable del CAP Raval Nord, CAP al que la titular de los datos estuvo inscrita durante unos años. No se trataba del CAP Drassanes, al que se había dirigido la petición, pero por lo que explicó durante la llamada que los dos centros compartían algunas gestiones o equipos responsables. El motivo de la llamada era indagar sobre cuáles eran los motivos por los que quería acceder a los datos, así como también pidió si es que había habido algún problema, si había tenido alguna experiencia negativa, o si lo estaba haciendo por motivos profesionales o personales. También pedía qué datos en concreto le interesaba saber si tenían. La persona que hizo la llamada pretendía una cierta normalidad en esta gestión pero resultaba bastante esperpéntica, ya que denotaba una inquietud y falta de normalidad por el hecho excepcional de precisamente llamar al teléfono móvil de la persona solicitante. Finalmente, unos días más tarde, recibimos por carta un acuse de recibo, y unos días después también otra carta informando de qué es la gestión de datos que llevan a cabo en función de la legalidad y políticas relacionadas y donde se anunciaba que adjuntaban documentos anexos, como la historia clínica, pero no había ningún archivo anexo. Pasados unos pocos días recibimos la misma carta, pero esta vez sí que con los archivos anexos.
Pasaportes y DNI (Cuerpo Nacional de Policía)
Envío de carta. No recibimos ninguna respuesta.
Oficina del Censo Electoral Envío de carta, en dos semanas recibimos una carta con la respuesta satisfactoria.
Banco de España
Enviamos la petición vía correo electrónico. El día después recibimos un acuse de recibo. Tres semanas después recibimos un aviso de ampliación del plazo a 2 meses para respondernos (lo recibimos de hecho en 3 correos

diferentes por parte de 2 direcciones remitentes diferentes), argumentando que la petición era muy poco concreta y que el Banco de España es un ente muy complejo: «en atención a la Complejidad que reviste la solicitud por la diversidad de tratamientos efectuados por el Banco de España y la falta de concreción de la solicitud». Hacia el final de este plazo recibimos respuesta. Y el día después recibimos una ampliación de la información proporcionada el día antes.
Registros policiales - Ministerio del Interior, Dirección General de la Policía
Enviamos la solicitud por carta postal. No recibimos respuesta.
Europol
Enviamos la solicitud y al cabo de casi dos meses, recibimos respuesta mediante una carta postal.
Control de fronteras - Schengen Information System
Enviamos un correo electrónico. No recibimos respuesta.
Instituto de Secundaria
Enviada la solicitud. No recibimos respuesta.
Sciences Po (París)
Petición hecha vía email. Después de 15 minutos obtenemos una corta respuesta del asistente informático automatizado, diciendo que las peticiones de acceso se envían automáticamente aquí y que contactemos a los servicios administrativos de Sciences Po, y proporcionan un email. Los contactamos y recibimos una respuesta automática que dice que actualmente los servicios administrativos están muy ocupados y que darán respuesta cuando puedan. No recibimos más respuesta.
UCL (University College of London)
Recibimos una respuesta automática: "Si has hecho una petición de acceso, por favor considera este correo como un aviso de recepción y deberías recibir una respuesta nuestra en los próximos 40 días" (40 días parece que está más allá del plazo de un mes que establece la ley). Posteriormente recibimos otro correo pidiendo un documento de identidad e información más específica sobre qué tipo de datos estamos pidiendo (si un documento específico, o la corresponencia de e-mails, y sino, que especificáramos los departamentos o los nombres de las personas que podrían tener datos de la persona interesada, así como si podíamos especificar un periodo de tiempo por el que estábamos buscando información).
Registro de licencias de conducción
Recibimos un correo electrónico donde se nos informaba de los datos que les constaban, en un documento claro y explicativo. En este caso remitimos la petición por vía postal, y recibimos la respuesta en digital a la dirección

de e-mail facilitada en la solicitud.
Programa Gaudir+ (Ajuntament de Barcelona)
Efectuamos una petición vía correo postal ya que no encontramos acceso a cómo hacerlo en la página web [actualmente hemos encontrado que puedes llegar a un formulario después de unos cuantos clics si visitas el apartado Aviso legal al pie de la página]. En todo caso, al enviar la petición, esta nos es devuelta con una respuesta diciendo que la solicitud no cumple los requisitos ya que se requiere adjuntar una copia del DNI y también piden que dada la gran cantidad de datos que existen en este organismo público, hay que especificar de qué datos se desea obtener información.

Sector privado

Twitter
Una vez rellenado y enviado el formulario, el mismo día nos envían un acuse de recibo. Al día siguiente envían un correo de respuesta, indicando cómo acceder a los datos. Respuesta rápida y satisfactoria.
Equifax
Envío de una solicitud vía correo electrónico. En menos de una semana envían un correo electrónico con la respuesta.
Experian
Envío mediante un correo electrónico, y dentro del plazo recibimos un correo de respuesta con un archivo cifrado con los datos solicitados, del que envían la contraseña en un segundo correo electrónico.
Tarjeta de fidelidad (tienda de comida)
Enviada la solicitud. No obtenemos respuesta. Se da la circunstancia de que la página web tiene un apartado dedicado a privacidad pero que no contiene la información sobre cómo ejercer los derechos ARCO (entre los que el derecho de acceso), también dice que facilita la política de privacidad pero donde debería haber un enlace o un archivo para descargar, aparece escrito entre paréntesis «es el otro archivo». Obviamente se trata de un error pero denota como hace falta afinar la política de datos de esta empresa.
Tarjeta de fidelidad (supermercado)

Al momento de hacer la petición nos resultó imposible de encontrar ningún contacto en su página web.
Operador de telefonía móvil
Envío de carta. No recibimos ninguna respuesta.
Registros bancarios
El formulario no aceptaba el código postal de España y no se pudo enviar.
Escuela privada de primaria
Enviada la solicitud, responden pidiendo ir en persona para identificarse.
Sage Publishing
Enviada la solicitud. Sin respuesta.
Facebook
Accedido, información correcta.

Microsoft
Accedido, información recibida correctamente.
Google
Hecha la petición online, recibimos el archivo con los datos el mismo día. Datos clasificadas en diferentes categorías, no demasiado útil.
Mozilla
Mes de julio del 2018. Imposible de encontrar un lugar donde ejercer derechos de acceso, a parte de una dirección en EEUU, aún y el marketing pro-privacidad de la compañía. No hay punto de contacto en ninguna parte.
Eurotunnel
Solicitud hecha vía correo electrónico. Respondieron enseguida diciendo que habían mirado a la base de datos y no habían podido encontrar nada de la persona solicitante. También pedían aportar información sobre qué

datos concretamente deberían tener, y si la persona titular de la solicitud podía proporcionar su documento de identidad, que sería borrado inmediatamente.
WhatsApp
Solicitud hecha vía web. Mediante un link se puede acceder a descargar los datos, que obtenemos sin problema en un informe completo al cabo de tres días.
Protonmail
Solicitud hecha vía email. El equipo legal responde el mismo día explicando donde se puede acceder a encontrar los diferentes tipos de datos y para qué fines los tienen. Especifican que los datos que se incluyen son siempre y únicamente los que ha introducido el usuario, y que esta información no es nunca compartida con terceras partes, excepto cuando lo requiere la ley Suiza (en casos de investigación).
Idealista
Enviamos la petición por correo electrónico y recibimos la respuesta dentro del plazo, en un formato de texto HTML nada fácil de leer. Explicaban sus obligaciones legales, y iban respondiendo a cada punto de una manera genérica que trataba de demostrar que cumplen la legalidad. De las respuestas más complicadas de leer que hemos recibido, aunque en definitiva se puede llegar a entender. Pero la presentación es muy desordenada.
Amazon
Petición enviada por correo electrónico. Envían respuesta el mismo día diciendo que podemos acceder a más información a través de las opciones de la configuración de la cuenta, con instrucciones: "If you require further personal data, you can log into your account to verify your identity and submit your request. You can submit this request through the “Contact Us” page in your Amazon customer account after logging in: https://www.amazon.co.uk/gp/help/customer/contact-us Once there, click on “Prime and more”, “Tell us more about your issue”, “request my data,” and follow the instructions."
Aparcaments Garví (parking privado)
Una vez hecha la solicitud, recibimos una carta solicitando el DNI, una vez lo enviamos recibimos otra carta donde se nos detallaban los datos personales que tienen de la persona titular que ha efectuado la petición. Una información proporcionada completa y correcta.
Partido político
Envío de una carta postal solicitando acceso a los datos. No recibimos respuesta.
Compañía de seguros
Recibimos una carta dentro del plazo contemplado por la ley que nos informa que nuestra petición de acceso no reúne los requisitos necesarios para acreditar la identidad de la persona afectada, y nos piden de hacerles llegar la petición con una fotocopia del DNI o permiso de residencia.