La movilidad y la ética de los datos

RAFAEL FERNÁNDEZ CAMPOS
Chief Data Officer, Bankia
Presidente, Club Chief Data Officer Spain

El uso masivo de datos que hoy permite la tecnología nos ha llevado a una paradoja interesante:

- Por un lado, donamos con gusto infinidad de datos personales a decenas de aplicaciones móviles, sin preocuparnos en exceso del uso que posteriormente harán de nuestros datos
- Por otro, nos escandalizamos cuando se publica una noticia según la cual nuestros datos van a ser empleados explícitamente para algún fin concreto, por muy lícito y encomiable que resulte

Dentro de las preocupaciones asociadas a los datos, podríamos diferenciar cuatro tipos: seguridad, privacidad, manipulación y ética del uso de los datos.

En el caso de la seguridad estamos hablando de actos desarrollados con un fin delictivo: robo de dinero, de datos, de identidad, estafa, extorsión, espionaje, ataques informáticos para bloquear páginas webs o pedir rescates...

Una vez hayamos conseguido una cierta invulnerabilidad de nuestros datos, el siguiente problema será el de la privacidad de los mismos. En este caso la preocupación proviene de la posibilidad de que nuestros datos personales sean hechos públicos o utilizados para fines que, aun dentro de la legalidad, constituyan una invasión de nuestra intimidad no aceptada por nosotros.

El grado de conocimiento que los grandes de la era digital tienen sobre nuestras vidas es abrumador. Se suele decir que con 150 *likes* nos conocen mejor que nuestros padres, y con 300 lo harán mejor que nuestras parejas. La preocupación social por este asunto provocó la creación de leyes que garantizaran la privacidad de nuestros datos, bien es cierto que, con relevantes diferencias entre países, incluso dentro del mundo occidental. No ofrecen las mismas garantías las leyes europeas que las norteamericanas, por no hablar, obviamente, del caso de países como China. Circunscribiéndonos a Occidente, hay que reconocer que, a pesar de todo, la sociedad aún no ha abierto plenamente los ojos a esta realidad, si bien los pasos son esperanzadores.

El tercer capítulo de preocupaciones proviene de los escándalos acerca de las *fake news* y su uso para torcer la voluntad de los votantes en países como Estados Unidos, Reino Unido e incluso España. No es lo peor la constatación de nuestra vulnerabilidad ideológica, sino la certeza de haber sido nosotros mismos los que hemos facilitado nuestra manipulación mediante la compartición de datos personales de forma voluntaria en las redes sociales. Esta toma de conciencia abre una puerta a la esperanza, ya que como decía Galbraith, "para manipular eficazmente a la gente es necesario hacer creer a todos que nadie les manipula".

La última de nuestras preocupaciones, la ética en el uso de los datos, es aún un asunto reservado a una minoría de conocedores de las implicaciones éticas del uso de las nuevas tecnologías. Hablamos de cuestiones como la discriminación de las minorías, el engaño, la promoción de adicciones, el comercio de datos, etc.

Ya son muchas las organizaciones que se han puesto manos a la obra para diseñar un decálogo de uso ético de los datos, desde organismos públicos a empresas privadas.

Quisiera repasar ahora los que en mi opinión constituyen los siete principios básicos de una ética digital, aplicados al caso de la movilidad:

Principio 1. La persona en el centro: el procesamiento de datos debe ir siempre en beneficio de aquellos de los cuales los hemos capturado y proteger su dignidad, integridad, libertad, privacidad y seguridad. Pensemos, por ejemplo, que el uso de los datos relativos a nuestra geolocalización debe repercutir en un bien para nosotros, en forma de optimización de recorridos, aumento de las posibilidades movilidad, etc. Si de ellos se benefician terceros, o nosotros nos beneficiamos de los datos de otros, pues mayor valor para el conjunto de la sociedad.

Principio 2. Control personal sobre los datos: los clientes o usuarios son los auténticos dueños de sus datos, por lo que siempre deben tener control total sobre ellos. Esto significa que si yo decido permitir el acceso a datos personales de cualquier tipo a aplicaciones que facilitan mi movilidad, debo poder en cualquier momento denegar dicho acceso, rectificar los datos inexactos o incompletos, hacer que se supriman mis datos personales, cancelar mi relación con la compañía, oponerme o limitar el tratamiento y ejercer mi derecho a la portabilidad.

Principio 3. Transparencia: tanto los datos almacenados, como el propósito para hacerlo, además del resultado de los procesos automáticos (algoritmos), deben ser transparentes y explicables para los intervinientes. Asimismo, la interacción con un sistema de Inteligencia Artificial debe ser previamente advertida. Si en algún momento interacciono con la aplicación, ya sea por voz o texto, debo ser advertido de que trato con un asistente artificial. De igual modo, los algoritmos sobre la base de los cuales se me ofrecen soluciones de movilidad deben ser explicables, un factor clave en la posibilidad de aplicación del siguiente principio.

Principio 4. Igualdad: el tratamiento de datos debe respetar el principio de igualdad, atendiendo especialmente a la protección de los sectores más vulnerables de la sociedad y a las grandes asimetrías en la información disponible, para evitar discriminación y estigmatización. Aunque suene distópico, no es difícil imaginar a un grupo de comerciantes elitistas de una calle muy concurrida, pagando a Google para que en los recorridos recomendados desvíen el tráfico lejos de su calle, y por tanto perjudicando a los comerciantes de otro lugar. O una aplicación de coches eléctricos compartidos, no permitiendo que los individuos de una determinada nacionalidad, o credo, o ideología, tengan acceso a sus vehículos.

Principio 5. Seguridad y privacidad: los datos deben estar siempre protegidos para garantizar la privacidad, desde el propio diseño de los procesos *(privacy-by-design)*. Sin seguridad no hay privacidad, y sin privacidad no hay ética. Los usuarios confiamos en que las compañías a las cuales cedemos nuestros datos personales dispongan de controles suficientes que garanticen la seguridad de los mismos. Asimismo, confiamos en que los tratamientos de datos no se extralimiten respecto a lo aceptado en las condiciones de uso. En este sentido, las compañías deberían realizar un esfuerzo sumplementario a la hora de simplificar las condiciones de privacidad que firmamos al darnos de alta en una aplicación y mejorar su comprensión por parte de los usuarios.

Principio 6. Responsabilidad: la compañía debe ser responsable del uso ético de los datos en todo su ciclo de vida, lo que conlleva implantar las medidas suficientes para garantizar dicho principio, diseñar productos y algoritmos éticamente responsables *(ethics-by-design)*, y velar porque los terceros participantes en nuestra cadena del dato cumplan nuestros estándares éticos. La privacidad y la ética no se improvisan, antes bien, obedecen a una intención, ya sea movida por la regulación o determinada por los ejecutivos. De ahí surge la estrategia de ética del dato de las empresas, que ha de contemplar unos objetivos generales y garantizar los procedimientos, responsabilidades y tecnologías necesarias para llevarla a cabo. Todo ello esponsorizado por la alta dirección. Imaginemos una aplicación que facilita la movilidad a través de diferentes tipos de vehículos, ya sean privados o públicos, pero que no se asegura de que la captura de los datos de las compañías suministradoras haya respetado sus estándares de privacidad y uso ético. Esto constituiría un alto riesgo reputacional que, aunque no es achacable directamente al tratamiento final, sí lo es de forma indirecta a través de los incumplimientos por parte de sus proveedores de datos.

Principio 7: Sostenibilidad: la ética del dato debe incardinarse en la estrategia global, de forma que sea perdurable y consustancial a la misión de la compañía, lo que supone el impulso de una cultura ética dentro de la organización. La ética en el uso de los datos supone un cambio de mentalidad en el uso de los mismos, que debe involucrar a toda la organización. Para ello han de habilitarse los mecanismos de gestión del cambio necesarios. La esponsorización es clave para la implantación de una cultura ética, pero la sostenibilidad de la misma solo se consigue mediante la persuasión y el convencimiento, por parte de toda la compañía, de la bondad de contar con unos sólidos valores éticos aplicables a la gestión de datos.

Para finalizar, quiero hacer mención al necesario equilibrio entre la privacidad de nuestros datos y la usabilidad de los mismos en beneficio de la sociedad y de nosotros mismos.

¿No queremos que, al salir de casa, haya un coche eléctrico disponible para trasladarnos al trabajo? ¿Y no quisiéramos que, al bajarnos del tren, nos estuviera esperando un patinete para poder recorrer los últimos metros hasta nuestro lugar de cita? ¿O que una app nos proponga el mejor modo de llegar a nuestro destino combinando diferentes modos de transporte? ¿O que nos diga los lugares de mayor atasco para tratar de evitarlos? ¿o que nos avise si vamos a llegar tarde a coger un vuelo?

Todo ello no puede hacerse sin que estas empresas conozcan dónde vivimos, dónde trabajamos, dónde empleamos nuestro tiempo de ocio, qué recorridos realizamos, etc.

No pensemos en compañías malvadas que buscan comerciar con nuestros datos con fines espurios, pues esto prácticamente no existe. Pensemos en compañías cuyo modelo de negocio se basa en solucionar problemas a la gente para, de esta manera, generar valor para la sociedad y, lógicamente, ser remunerados por el riesgo asumido y la gestión realizada.

Aunque haya alguna compañía que se comporte irresponsablemente, no debemos generalizar, ya que el primer y mayor reto de las empresas es la supervivencia, y cada vez más esta es impensable sin unos valores éticos sólidos, sin los cuales será la misma sociedad las que las expulse del mercado y las haga desaparecer.