Andromeda Value sobre el escándalo de Facebook

NOTA DEL EDITOR: *Este comentario supone un extracto de la carta trimestral recientemente publicada a los partícipes de Andromeda Value Capital.*

* * *

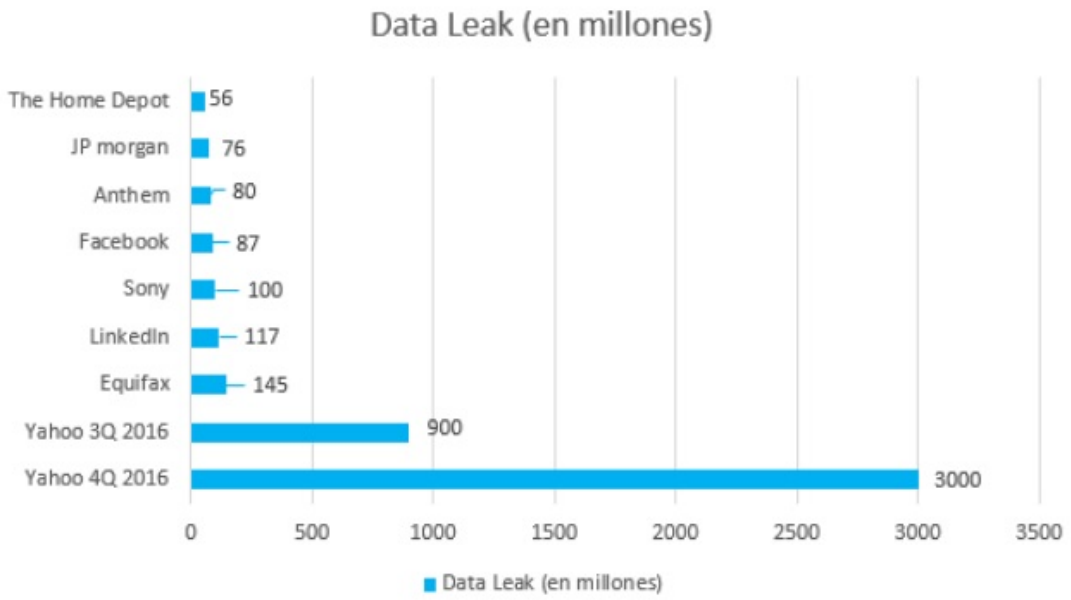
Por poner en contexto: **Facebook** ha sufrido una caída de cierto peso en la cotización de sus acciones debido al escándalo de Cambridge Analytica. Básicamente, lo que la opinión pública ha entendido es que los datos de millones de usuarios de Facebook han sido explotados por esta compañía (Cambridge) para influir en las elecciones americanas y favorecer la victoria de Trump.

En nuestro análisis vamos a explicar dos cosas. En primer lugar, la gestión de las crisis y, en segundo lugar, porque esta idea que se ha transmitido a la opinión pública es terriblemente errónea.

A lo largo de la vida de una compañía cotizada existe un riesgo de entre un 15% a un 20% de que algún tipo de escándalo le salpique. De modo que, este tipo de crisis son extremadamente frecuentes. Lo importante sobre todo en estos casos es la gestión de cómo se llevan a cabo.

En 1982 **Johnson & Johnson** sufrió la crisis del Tylenol (alguien envenenó pastillas en el proceso de producción). En 1990 el agua Perrier sufrió otro caso de envenenamiento de producto. En 1993 una jeringuilla apareció dentro de una lata de Pepsi. En 2009 **Toyota** tuvo que afrontar un recall masivo de vehículos debido a fallos en el acelerador. En 2012, 5 niños murieron por consumo excesivo de la bebida Monster, producto de Monster Beverages. En 2014 **McDonald´s** y **Yum Brands** (dueña de KFC) vieron como a sus filiales en China les suministraban carne de vacuno en mal estado. En 2016 un piloto de **Lufthansa** estrelló un avión lleno de pasajeros en los Alpes. E innumerables casos más.

O solo por centrarnos en compañías que han sufrido una filtración de datos, aquí tenemos una recopilación con la gravedad de estas. Y en la mayoría de los casos no ha supuesto problema alguno al negocio.



Todos estos casos, a diferencia de aquellos catalogados como fraudes, donde las empresas eran conscientes del mal comportamiento que estaban llevando a cabo, se acabaron solucionando con un ataque directo al problema y cierta paciencia en el tiempo. El caso de Facebook cumple los principios de lo expresado anteriormente y en un par de trimestres, (de no salir nueva información) este asunto se habrá olvidado. Lo cual no quita que la gente no siga dándose de baja de la red social Facebook, pero eso ya es más por una cuestión de lo tóxica que se ha vuelto la plataforma en estos momentos, la cual ha mutado a algo semejante a un bazar turco, donde la experiencia de usuario se ha convertido en lamentable. Sin embargo, sigue existiendo Instagram y los crecimientos no deberían suponer un problema, considerando a lo que cotiza la acción.

Por otro lado, está la explicación de lo acontecido y lo terriblemente mal que se ha entendido.

Facebook jamás sufrió un hackeo, sino que los datos se extrajeron del programa de APIs que se implantó en 2010. Una APIs (interfaz de aplicación de programas), informáticamente hablando, es como la pestaña de una pieza de puzzle que permite casarla con otra pieza, para que el puzle se pueda completar. Es decir, cuando desarrollamos una aplicación informática necesitamos cosas que puedan completarla y que no requieran escribir nuevas líneas de código. Porque de no ser así el proceso de codificación sería inviable. Habría que escribir líneas y líneas de código de las cuales podemos no tener ni idea. Por ejemplo, desarrollamos una aplicación móvil que nos indique cual sería el local comercial óptimo para el tipo de negocio que estamos haciendo crecer, es decir, metros cuadrados y ubicación. Pero además del sistema que nosotros hayamos creado para optimizar esta búsqueda seguro que necesitamos la información de Google Maps. Pues bien, utilizaríamos las líneas de código de Google Maps para integrarlas en nuestra aplicación. Esas líneas de Google Maps las obtendríamos a través de la propia API de Google Maps.

Sabiendo esto, Cambridge jamás hackeó Facebook, sino que los datos los extrajo de una de las APIs de Facebook que permitían obtener dichos datos. Igual que cualquier otra aplicación pudo obtenerlas. Realmente no hubo robo de datos. De hecho, Facebook posee datos que no suministra a terceros a través de APIs. Pero justo estos datos sí que eran de los suministrados. El problema, es que conforme la política de Facebook, estos datos no se pueden revender ni emplear incorrectamente. Cosa que sí hizo Cambridge. Pero evidentemente Facebook falló en controlar la mala gestión de datos que hacían terceros. Y este precisamente es el problema de Facebook, que si deberían haber prestado atención a esas malas prácticas. Tanto es así, que se sabe que hay un mercado negro de datos de Facebook. Es más, solo hay que entrar en alguna web oscura por medio de Tor o I2P, para saber que esto existe y que dichos datos se explotan inmoralmente. Igual que se trafica con armas o droga.

Pero es que esto no deja de ser un mal mayor de la población debido a sus escasos conocimientos de ciberseguridad. Que cuando se enteran de los hechos se escandalizan... Nuestros datos están masivamente comprometidos constantemente. Aunque si tanto preocupan cuánto valen de media vuestros datos en Facebook os diremos que simplemente unos 82 dólares...

Por otro lado, está el argumento de que Cambridge ayudó a aupar al poder a Trump. Dudamos que esto sea así debido a la complejidad del asunto. La teoría del caos apunta un poco en esta dirección. Para entornos tan dinámicos como unas elecciones generales la idea de que un solo factor es el determinante lo reduce todo a una proposición demasiado simplista. Además, Ted Cruz, otro de los candidatos republicanos también empleó a Cambridge con anterioridad a que lo hiciese la administración Trump y el resultado fue de derrota.

En cualquier caso, lo que todo esto parece apuntar es a una mayor regulación en cuanto a los datos. En Europa ya se está imponiendo el reglamento GDPR y mundialmente posiblemente vayamos a algo similar. Al final, lo que esto genera es precisamente contra-intuitivo del miedo de los inversores.

La comunidad financiera cree que una mayor regulación perjudicaría a negocios como Facebook. Precisamente lo contrario. La regulación suele consolidar a los “incumbents” (los negocios ya establecidos). Puesto que Facebook ya tiene todos nuestros datos. De modo que lo que generas en un *lock-up* (encerramiento), impidiendo que terceros puedan acceder a ellos y desarrollarse. Es decir, la era de las grandes redes sociales ya se ha acabado. El miedo a que una nueva red social aparezca y desbanque a Instagram desaparece al producirse este “encerramiento de datos”, sencillamente porque las redes sociales necesitan la conexión de amigos y gustos para extenderse. Pero si ahora ya no puedes acceder a esos amigos y gustos de Facebook, sino que los tienes que descubrir tu sólo como app, la dificultad es terriblemente mayor. La gente no se va a tomar el tiempo de enseñar a las apps que quieren o que les gusta y lo que acabas produciendo es que dediques más tiempo a aquellas que ya te conocen. El nuevo Facebook o el nuevo Instagram son el antiguo Facebook y el antiguo Instagram con funciones nuevas. Pero el miedo de que Facebook sea como MySpace no va a ocurrir.

Lo único que podría desbancar a Facebook frente a una nueva red social sería aquella que se basase en una nueva tecnología, por ejemplo, realidad aumentada. Y aun así Facebook tendría la fuerza económica para copiarla o comprarla. Y necesitas que ese salto tecnológico se dé...cosa que no es sencilla. MySpace, Fotolog o Windows Messenger sencillamente murieron porque nunca conocieron el Big Data, que fue precisamente el salto tecnológico

que las mató.