Digital Future Society

Privacy-first:

Un nuevo modelo de negocio para la era digital

Un programa de

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
MOBILE WORLD CAPITAL BARCELONA

Digital Future Society

Sobre Digital Future Society

Digital Future Society es una iniciativa transnacional sin ánimo de lucro que conecta a responsables políticos, organizaciones cívicas, expertos académicos y empresarios para explorar, experimentar y explicar cómo las tecnologías se pueden diseñar, usar y gobernar, a fin de crear las condiciones adecuadas para una sociedad más inclusiva y equitativa.

Nuestro objetivo es ayudar a los responsables políticos a identificar, comprender y priorizar los desafíos y las oportunidades fundamentales, ahora y en los próximos diez años, en relación con temas clave que incluyen la innovación pública, la confianza digital y el crecimiento equitativo.

Para más información visite digitalfuturesociety.com

Un programa de

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL BARCELONA

Publicado
Marzo de 2020.

Aviso legal
La información y las opiniones expuestas en este informe pertenecen al autor(es) y no reflejan necesariamente la opinión oficial de Mobile World Capital Foundation. La Fundación no garantiza la exactitud de los datos incluidos en este informe. Ni la Fundación ni ninguna persona que actúe en nombre de la Fundación será considerada responsable del uso que pueda darse a la información que contiene.

Nota a la versión en español
Este informe ha sido escrito en inglés y traducido al español. Digital Future Society apoya el uso de conceptos técnicos en español y se esfuerza por encontrar una traducción precisa, siempre que sea posible, sin comprometer por ello el significado original del contenido.

Digital Future Society

Contenidos

Resumen ejecutivo

Los datos, que antes eran sólo un subproducto de la transformación digital, se han convertido en el principal motor del desarrollo tecnológico moderno. Aunque el análisis de datos aporta nuevas posibilidades para los gobiernos, las empresas y los ciudadanos, la generalización de los modelos de negocio basados en extracción y el tratamiento de datos genera cada vez mayor inquietud.

La proliferación de plataformas digitales y dispositivos con conexión a Internet ha contribuido a que los métodos de extracción de datos sean cada vez más sofisticados, especialmente en lo que respecta a los datos personales. En 2018 se acuñó el término *surveillance capitalism* (capitalismo basado en la vigilancia) para referirse al carácter invasivo de esas prácticas comerciales y la amenaza que suponen para la privacidad de las personas e incluso para la sociedad tal como la conocemos.

Los gobiernos de todo el mundo se enfrentan a la compleja tarea de encontrar un equilibrio entre facilitar el flujo de datos para fomentar el crecimiento económico, por un lado, y proteger la privacidad de los ciudadanos por el otro. Conscientes de este delicado equilibrio, las Naciones Unidas reclaman "un debate en toda la sociedad, basado en el consentimiento informado, sobre qué límites y normas habría que aplicar a esos usos en la tecnología digital y la IA".[1]

Las leyes sobre el tratamiento de los datos, como el Reglamento General de Protección de Datos (RGPD), apenas empiezan a dar fruto y tanto los expertos jurídicos como los especialistas en materia de protección de datos reconocen que las normas no pueden ir más allá en la preservación de la privacidad real. La nueva legislación, sumada al llamado *techlash* (la creciente desconfianza en las empresas tecnológicas), han provocado la aparición de un nuevo modelo de negocio basado en dar prioridad a valores fundamentales como la privacidad, la confianza y la transparencia por encima del beneficio y el crecimiento empresarial. Este informe se refiere a estos negocios como modelos *privacy-first*. Estos nuevos modelos de negocio, que siguen siendo minoritarios, desafían el paradigma de extracción de datos que actualmente impulsa la economía digital.

Aunque el mercado necesita modelos que anteponen la privacidad, estas empresas se enfrentan a un sinfín de barreras. Sus principales competidores son empresas basadas en plataformas digitales que controlan el mercado y se benefician de los efectos de red. La escasa financiación y el lento crecimiento de estos negocios dificultan aún más que puedan aprovechar el potencial de su propuesta de valor.

Los gobiernos pueden implementar medidas que incentiven su crecimiento, sobre todo porque estas empresas son una excepción en la industria tecnológica. Además de dar a conocer su existencia y describir las oportunidades y los desafíos que plantean los modelos *privacy-first*, el presente informe es una invitación a los responsables de formulación de las políticas a que vayan más allá de la regulación y se comprometan con estos modelos que construyen una economía digital basada en la confianza, la transparencia y la privacidad.

Este informe se basa en las conclusiones del grupo de trabajo sobre confianza y seguridad digital del Digital Future Society Think Tank. Va dirigido a los responsables de formulación de las políticas y presenta una visión general de este nuevo modelo de negocio. Analiza cuatro ejemplos de empresas ya existentes que se ajustan a este modelo y son rentables. El informe concluye con tres propuestas que los responsables políticos pueden aplicar para abordar los desafíos y aprovechar las oportunidades que plantean y, a la vez, crear nuevas oportunidades.

[1] Digitalcooperation.org 2019

Glosario

Capitalismo basado en la vigilancia

Acuñado por la psicóloga social Shoshana Zuboff, este término se refiere a un mercado en el que las grandes empresas tecnológicas recopilan datos sobre el comportamiento de los usuarios con fines comerciales, lo que puede tener importantes -y a veces graves- consecuencias como el control y el seguimiento de la sociedad, tanto por parte de entidades públicas como privadas.[2]

Cebra

En el ecosistema de las startups, las cebras simbolizan un modelo de negocio y un conjunto de valores totalmente contrarios a los representados por los unicornios. El término surge de un movimiento liderado por varias mujeres empresarias con el objetivo de "crear alternativas" al status quo de la cultura de las empresas emergentes.[3] Estas empresas se fundamentan en principios como el crecimiento sostenible, la cultura no discriminatoria y un enfoque ético de los negocios.

Código abierto

Cuando el software es de código abierto, su código fuente es público. Este término también alude a un enfoque empresarial más participativo y democrático que el de los proyectos basados en licencias privadas. Cualquier usuario puede modificar o compartir el software de código abierto, con cualquier finalidad. La distribución de este código debe ser totalmente gratuita, no discriminatoria y tecnológicamente neutral.[4]

Dependencia del proveedor

Estrategia comercial de algunas empresas que consiste en dificultar el derecho del cliente a cambiar a una tecnología o producto alternativos de otro proveedor. Cambiar de proveedor suele implicar una gran inversión en tiempo y dinero. Esta práctica, que limita la competencia en el mercado, se ha extendido en los últimos años a sectores como los servicios de almacenamiento de datos.[5]

Economía de plataforma

La economía de plataforma engloba todas las plataformas digitales que actúan de intermediarias entre los usuarios y las empresas que ofrecen servicios. Esta definición incluiría a las plataformas que facilitan transacciones comerciales, como Amazon o Uber, pero también a los entornos tecnológicos que permiten el desarrollo de negocios digitales.

[2] Couldry 2016

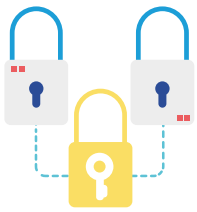
[3] Brandel et al 2017

[4] Opensource.org 2019

[5] Schacklett 2018

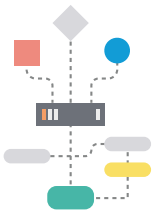
Efecto de red

En términos económicos, el efecto de red se refiere al fenómeno por el cual un mayor número de usuarios o clientes aumenta el valor de un bien o servicio. Su alcance viene definido por cuestiones como la calidad o la utilidad del producto, su precio o el conocimiento de la marca. Para las plataformas digitales o las redes sociales suele ser un factor de éxito crucial.



Encriptación

La encriptación es un método que codifica un mensaje o información con el fin de ocultar su contenido o significado. Para descifrar el contenido del mensaje se requiere una clave o contraseña que lo descodifique y dé acceso al contenido. Se trata de una técnica que se utiliza habitualmente para aumentar la seguridad en cualquier tipo de comunicación digital.

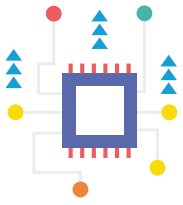


Extracción de datos

Proceso de recopilación de datos de distinto origen, como la actividad del usuario en Internet. Para las empresas con un modelo de negocio basado en la monetización de datos, este es el primer antes de analizar, procesar y obtener beneficios con esa información.

Intermediario de datos

Un intermediario de datos es cualquier tipo de entidad que recaba, recopila y comercializa datos personales, derivados o inferidos de diverso origen, público o privado.[6]



Nube descentralizada

Una red de múltiples dispositivos conectados en la que se almacenan datos e información anónima. Este modelo es una alternativa a las grandes empresas de almacenamiento de datos en la nube, que pueden entrañar varios riesgos (control por parte de empresas privadas, amenaza de fugas masivas, infraestructura vulnerable, etc.) para la seguridad y la privacidad de los datos.

[6] Nytimes.com 2019

Privacidad desde el diseño

Este concepto, desarrollado por Ann Cavoukian en la década de 1990, es un marco que aborda los efectos sistémicos y en constante crecimiento de las tecnologías de la información y la comunicación, las prácticas comerciales y los sistemas de datos en red a gran escala.

Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos sustituyó a la Ley de Protección de Datos en 2018. El objetivo del RGPD es facilitar un conjunto de normas de protección de datos a los distintos Estados miembros de la Unión Europea y el Espacio Económico Europeo (EEE).[7]

Unicornio

En la industria del capital de riesgo, un unicornio es una empresa emergente valorada en más de 1.000 millones de dólares. Conlleva un crecimiento exponencial de usuarios y una gran capacidad de generar ingresos rápidamente. Entre los unicornios más conocidos se encuentran Airbnb, Uber, Ant Financial y SpaceX.

[7] lapp.org 2019

Introducción

La economía de datos

International Data Corporation estima que los ingresos globales de los negocios que se dedican a explotar las aplicaciones de *big data* y a analizar datos alcanzarán los 274.300 millones de euros en 2022.[8] Estos datos ofrecen infinitas aplicaciones posibles a las empresas, por lo que a los políticos, los académicos y la sociedad en general cada vez le preocupan más las tendencias monopolísticas de las empresas tecnológicas y sus prácticas invasivas a la hora de obtener datos personales.

Por la propia naturaleza de la recopilación de datos online, ciertos tipos de empresas están mejor diseñadas que otras, por lo que son más proclives a beneficiarse de las oportunidades que ofrecen. Se trata de plataformas de servicios que han experimentado un gran crecimiento y se benefician de los efectos de red. Parte de la ventaja competitiva se debe a la capacidad de crear grandes conjuntos de datos.[9]

A partir de los datos obtenidos mejoran su oferta basándose en el análisis y en las conclusiones obtenidas, lo que consolida aún más su posición de liderazgo en el mercado. Ciertas plataformas de servicios como Google, Facebook y Amazon rentabilizan el valor de los datos ya que los conservan a lo largo de toda su cadena. Persiguen constantemente mantener el dominio del mercado y acumular conjuntos de datos cada vez mayores, lo que las ha llevado a crear un ecosistema que utiliza los datos como una nueva forma de capital económico basado en la acumulación y la circulación constantes.[10]

Los datos abarcan información generada tanto por máquinas como por seres humanos; sin embargo, ciertos modelos de monetización de datos conllevan un riesgo: acabar considerando al usuario una fuente de datos gratuita. El usuario como "materia prima" es un tema recurrente en los modelos de negocios digitales disruptivos. Estos modelos no sólo predicen el comportamiento de los consumidores, sino que tratan de maximizar los beneficios utilizando los datos para influir y modificar el comportamiento de los usuarios.

La psicóloga social Shoshana Zuboff ha llamado a este modelo "capitalismo basado en la vigilancia" (*surveillance capitalism*), un sistema en el que cada uno de nuestros movimientos alimenta predicciones sobre lo que haremos a continuación y en el futuro. Según Zuboff, la sociedad corre el riesgo de dividirse en dos grupos: los que vigilan y los que son vigilados, lo que supondría una nueva forma de desigualdad social "intrínsecamente antidemocrática".[11]

[8] International Data Corporation 2019

[9] GSMA 2018

[10] Sadowski 2019

[11] Naughton 2019

La creciente preocupación por la privacidad

Aunque los defensores de la privacidad en Internet han existido desde la mercantilización de la red, ahora son más visibles que nunca. Las filtraciones y violaciones de datos han provocado que el público sea más consciente de cultura de la vigilancia. La creciente concienciación sobre la importancia de los datos personales en los negocios digitales y la erosión de la privacidad de las personas han provocado que la preocupación por la privacidad, antes reducida al ámbito de la cultura hacker, se extienda a la sociedad en general. Este cambio se evidencia en una declaración de octubre de 2018 del CEO de Apple CEO, Tim Cook:

> **Nuestra información personal, desde lo cotidiano hasta lo más íntimo, se ha convertido en un arma que se utiliza contra nosotros mismos con precisión militar. (...) Cada día, se mueven miles de millones de dólares y se toman innumerables decisiones en base a nuestros gustos, amigos y familiares, relaciones y conversaciones, deseos y miedos, esperanzas y sueños. (...) Esos datos, inofensivos por separado, son cuidadosamente combinados, sintetizados, analizados, comercializados y vendidos. Llevado al extremo, este proceso crea un perfil digital permanente de cada uno de nosotros y permite a las empresas conocernos mejor de lo que nos conocemos a nosotros mismos.**[12]

La mayor concienciación de los consumidores abre una oportunidad que las tecnologías orientadas a la privacidad pueden aprovechar. Están surgiendo una serie de empresas que comparten una filosofía basada en la protección de los datos de los usuarios y que han tomado la decisión consciente de renunciar a los posibles beneficios derivados de la explotación de datos personales. Al hacerlo, estas empresas renuncian a un modelo que es sumamente lucrativo en el contexto actual de la economía de datos y la creciente extracción de información.

Acerca este informe

El objetivo de este informe es ayudar a los responsables políticos a identificar modelos de negocio cuyo valor fundamental es la privacidad y estudiar cómo se puede incentivar su crecimiento. El informe se refiere a estos modelos de negocio como *privacy-first*, es decir, negocios que anteponen la privacidad y no requieren de la extracción de datos, ya que no monetizan los datos personales.

El contenido de este informe se basa en el trabajo realizado por un grupo de seis expertos internacionales, que se reunieron durante dos días y medio en Barcelona en septiembre de 2019, y también en la investigación documental.

El informe comienza con una visión global sobre el origen de los modelos de negocio de extracción de datos y después explica brevemente algunas de las herramientas digitales que conforman el ecosistema de la privacidad y que enmarcan este informe: los modelos de negocio *privacy-first*.

[12] Asher Hamilton 2018

A través del análisis de cuatro empresas rentables con modelos *privacy-first*, el informe examina los desafíos y oportunidades que tienen ante sí al tratar de competir con los líderes del mercado que sí se benefician de la extracción de datos de usuarios a cambio de servicios "gratuitos". Estas empresas comparten una serie de rasgos, descritos en el anexo, que pueden servir de instrumento para que los responsables políticos las identifiquen con modelos *privacy-first*.

La última sección expone las iniciativas propuestas por el grupo de trabajo. Explica las distintas propuestas y cómo los responsables políticos podrían apoyarse en ellas para fomentar empresas basadas en valores. Las tres iniciativas incluidas en el informe abordan las oportunidades y los desafíos que se plantean las empresas *privacy-first*.

Destinatarios

El presente informe está dirigido principalmente a responsables de formulación de políticas. Su objetivo es ofrecer una visión global a quienes trabajan dentro de la administración pública, en cualquier lugar del mundo, y deben redactar o implantar normativas, marcos reguladores y reglamentos relacionados con la tecnología, en particular si forman parte de programas de innovación y contratación pública. Este informe también podría ser de utilidad para aquellas instituciones que abogan por una gestión justa de los datos. Por último, podría resultar de gran ayuda en lugares con escasa regulación de la gestión y la protección de los datos, ya que las propuestas podrían ser muy útiles a la hora de adaptar las políticas de gestión y protección de datos.

Alcance

¿Por qué nos centramos en los modelos de negocio *privacy-first*?

Los modelos de negocio *privacy-first* se oponen a los de extracción de datos o de capitalismo basado en la vigilancia. El informe analiza los modelos de negocio de estas empresas, así como sus prácticas de gestión de datos. Estas empresas son el vivo ejemplo del modelo de privacidad desde el diseño (PdD) definido en el RGPD.

El informe reconoce las limitaciones tanto de la legislación como de los principios de PdD. Las opiniones críticas señalan la ambigüedad de ambos y destacan la necesidad de definir metodologías que permitan acortar las distancias entre la teoría y la práctica. Queda mucho camino por recorrer ya que la sociedad aún no percibe el impacto de la legislación en las empresas y la ciudadanía. Al limitar el alcance de este informe a los modelos empresariales que han logrado priorizar la privacidad sobre el beneficio pretendemos ofrecer ejemplos sobre cómo llevar conceptos abstractos a la práctica.

¿De qué tipo de datos hablamos?

Este informe se basa en la definición de datos personales del reglamento RGPD: toda información pública o privada que pueda rastrearse o utilizarse para identificar a una persona, directa o indirectamente, por ejemplo, rasgos culturales, fisiológicos o sociales.

La gobernanza de datos es un asunto muy complejo[13], por lo que el análisis en profundidad de las limitaciones de la legislación a escala mundial queda fuera del alcance de este informe. El RGPD sirve de punto de partida para entrar en el debate. Este reglamento sobre datos es un hito, pero en el informe se destaca que, aunque protege mejor los datos de la ciudadanía que otras leyes, tiene sus limitaciones. Hay que tener en cuenta, además, que las empresas *privacy-first* seleccionadas para el informe tienen su sede en Europa y Estados Unidos, por lo que este tipo de empresas podrían tener un mayor impacto en mercados de países con leyes de protección de datos más permisivas.

Dado que la documentación relativa a la gobernanza de datos, la cadena de suministro de datos y las normativas es muy extensa, este informe no se centra tanto en el debate sobre la regulación como en los incentivos. Los incentivos propuestos al final del informe, que reconocen el valor y las limitaciones de la reglamentación, están concebidos para complementar la normativa ya se viene aplicando en todo el mundo.

[13] Ver Digital Future Society informe Hacia una mejor gobernanza para todos 2019

1

En contexto: los modelos de negocio basados en datos

¿Cómo hemos llegado hasta aquí?

El modelo de monetización de datos tiene su origen en los primeros tiempos de Google. Hasta entonces, los datos se usaban únicamente para mejorar la calidad de los productos, sobre todo la experiencia del usuario. Utilizados así, los datos eran un activo para compañías como Apple, cuyos ingresos dependían del hardware. Sin embargo, un motor de búsqueda como Google obtenía poco rendimiento de la inversión aunque ofreciera una mejor experiencia de búsqueda a los usuarios. Presionado por la necesidad de conservar a los inversores y sobrevivir como empresa, Google encontró una forma de obtener ganancias gracias a la gran cantidad de datos sobre el comportamiento de los usuarios que había recopilado: la publicidad dirigida.[14]

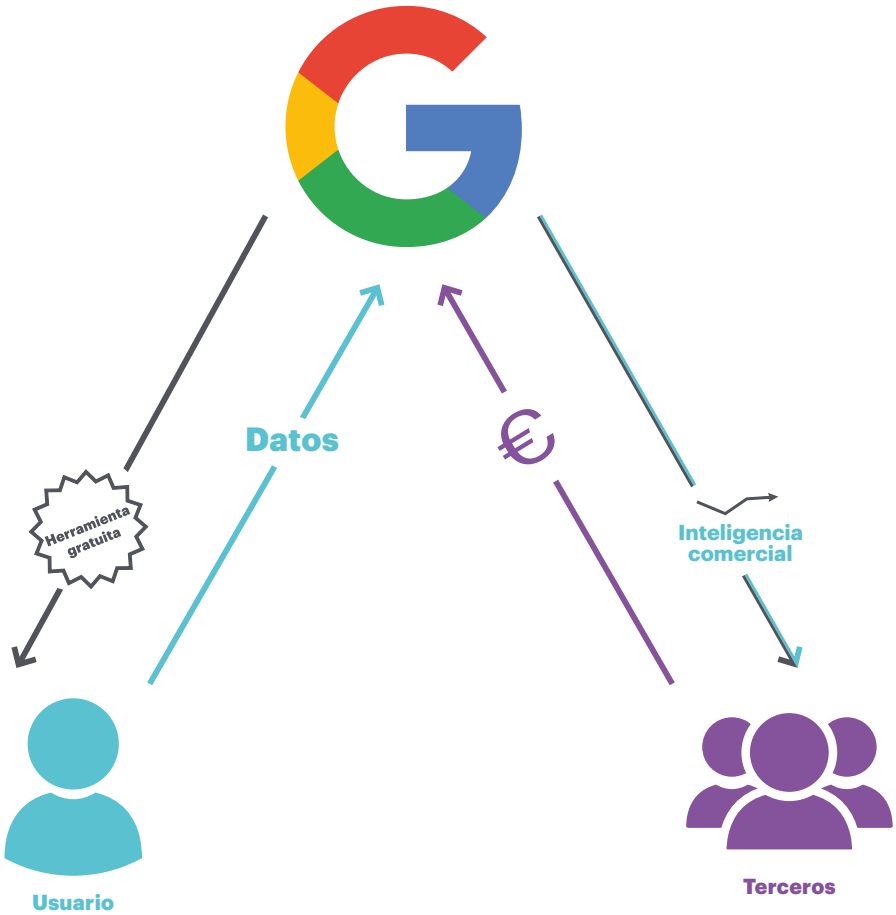


Ilustración 1: modelo comercial basado en monetizar los datos de usuario. Las búsquedas en Google recopilan todo tipo de datos sobre los usuarios: términos de búsqueda, resultados visualizados, lugares, idiomas, etc. Posteriormente, Google ofrece a terceros la posibilidad de personalizar la publicidad y prever la demanda.

Origen de la imagen: adaptada de Business Model Toolbox

[14] Zuboff 2019

Desde que Google recurriera a ella por primera vez, la monetización de datos ha evolucionado y se ha expandido a otros sectores. Además, los avances tecnológicos hacen más fácil la obtención de datos e impulsan el potencial económico de los modelos de monetización. La recopilación de datos, junto con el auge de los dispositivos móviles, los dispositivos inteligentes, el Internet de las cosas (IdC) y las redes sociales, han contribuido a crear modelos de negocio más sofisticados.

Cuatro grandes tendencias que impulsan el crecimiento de modelos de negocio basados en la monetización de datos

1	**Auge de las plataformas**	Los avances en aprendizaje automático y los potentes cálculos computacionales, respaldados por infraestructuras a gran escala, permiten la acumulación de los datos obtenidos.
2	**Aumento del uso de móviles**	Los móviles y las aplicaciones de los smartphones facilitan la obtención de datos de ubicación y comportamiento mediante el rastreo.
		Se espera que en 2025 el 71% de la población mundial tenga un móvil.[15]
3	**Nuevas formas de obtener datos con el IdC**	Mayor volumen de datos susceptibles de ser comercializados gracias a los dispositivos wearables, los dispositivos inteligentes, etc.
4	**Popularidad de las redes sociales**	La inferencia de perfiles de usuario, a través de los datos personales, ha abierto un abanico de oportunidades para los negocios, la educación, la política y la sociedad.

Ilustración 2: cuatro grandes tendencias que impulsan el crecimiento de modelos de negocio basados en la monetización de datos.

Origen de la imagen: Digital Future Society

Origen del contenido: Digital Future Society, GSMA

[15] GSMA 2018

Extraer valor de los datos

A la hora de monetizar los datos, un factor decisivo es si la empresa tiene la capacidad de analizar los datos internamente. Las que no tienen la infraestructura o los conocimientos técnicos necesarios pueden autorizar a los clientes a acceder a los datos en bruto a través de una licencia. La concesión de licencias de datos fue la estrategia de Twitter hasta 2010.[16]

Las empresas que poseen la infraestructura interna y los conocimientos técnicos en materia de explotación de datos suficientes ofrecen una gran variedad de servicios capaces de generar ingresos, como la publicidad dirigida, la anticipación de la demanda o los servicios de tarificación dinámica. Amazon, por ejemplo, utiliza datos obtenidos de las compras, las opiniones sobre productos y la ubicación. A partir de ellos ofrece servicios de consultoría a terceros, estimaciones de la demanda y tendencias. Una posible inferencia podría ser, por ejemplo, dónde debería construir su próximo almacén un proveedor.[17]

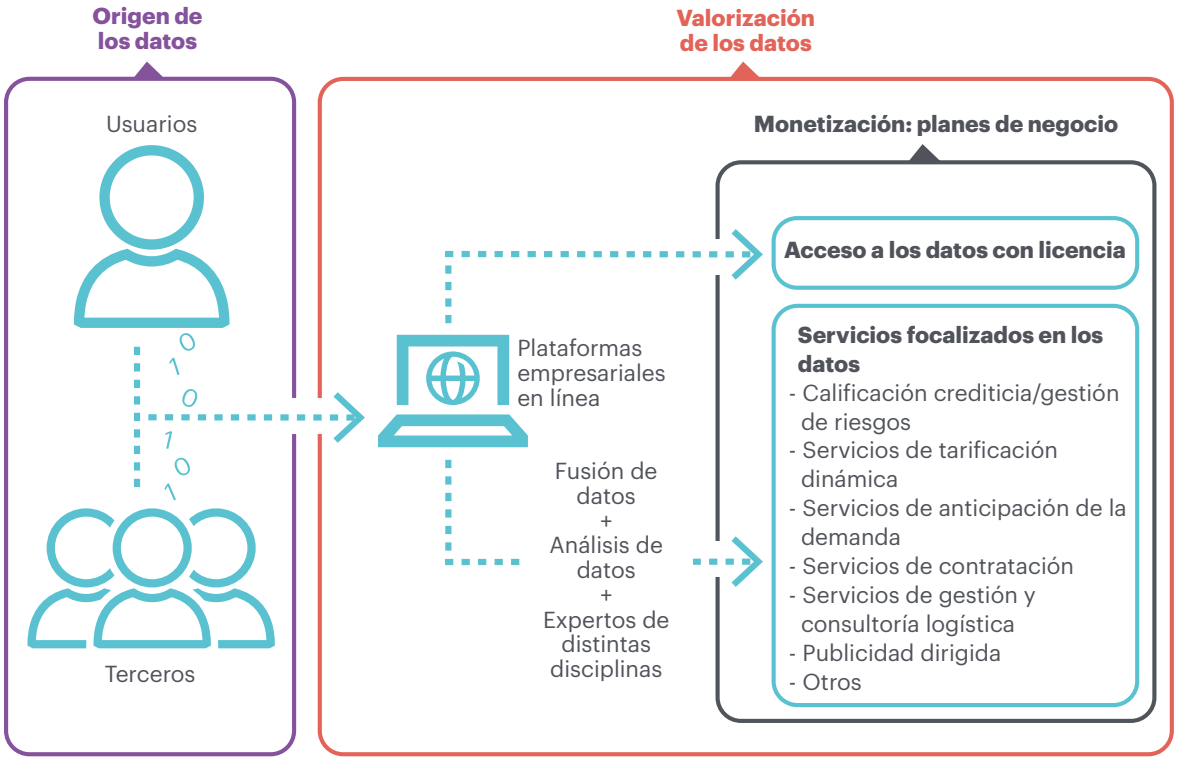


Ilustración 3: cadena de valor de los datos.

Fuente de la imagen: Ly et al.

[16] Ly et al. 2019

[17] Ibid.

A qué riesgos nos enfrentamos

Según la experta en privacidad Ann Cavoukian, el riesgo del modelo de negocio de extracción de datos es doble: estas prácticas no sólo ponen en peligro los derechos de privacidad de los consumidores expuestos a fugas de datos y ciberataques, sino que también amenazan la propia integridad de la empresa.[18]

La inquietud se ha extendido por todo el mundo. En un informe reciente de Naciones Unidas se destaca la urgencia de restablecer la confianza y garantizar el derecho a la intimidad, amenazado por los nuevos métodos de vigilancia, seguimiento y control de la ciudadanía.[19] Para ello propone un "un debate en toda la sociedad, basado en el consentimiento informado, sobre qué límites y normas habría que aplicar a esos usos en la tecnología digital y la IA".[20]

Además de poner en peligro la privacidad, los modelos comerciales de extracción de datos suponen una amenaza para la competencia y la innovación en el mercado. El crecimiento de las plataformas digitales y la importancia de los datos ha llevado a que la influencia y el poder se concentren en un número reducido de empresas.[21] A falta de una regulación nacional y mundial, los líderes del mercado son quienes dictan las normas sobre la disponibilidad y el uso de los datos, lo que afecta directamente a la competitividad de otros actores más pequeños en la economía de los datos como las pymes.[22]

La gobernanza de los datos y sus limitaciones

En el momento de redactar el presente informe, más de 100 países tenían leyes o reglamentos de protección de datos en vigor.[23] Aunque algunos líderes económicos y políticos temen que la implantación de estas leyes obstaculice la innovación, el rechazo se ha ido diluyendo tras el escándalo de Cambridge Analytica. No obstante, el debate sigue dividido entre quienes son conscientes de los riesgos para la privacidad que entrañan los modelos de monetización de datos y quienes tratan de establecer políticas que faciliten el flujo de datos a nivel mundial. Estos últimos seguramente tratarán de fomentar modelos de negocio que invadan la privacidad, de manera que los modelos que anteponen la privacidad cobrarán aún más importancia a la hora de construir un futuro basado en la confianza y la transparencia.[24]

Por lo que respecta a los reglamentos de protección de datos, los gobiernos de todo el mundo se han enfrentado a una serie de retos y oportunidades al intentar elaborar políticas que protejan la privacidad y los derechos de la ciudadanía en entornos digitales. Uno de los casos más destacados (por la magnitud del mercado al que afecta) es el RGPD de la Unión Europea.

[18] Jones 2018

[19] Digitalcooperation.org 2019

[20] Ibid.

[21] Faravelon et al. 2015

[22] Un.org 2019

[23] Unctad.org 2019

[24] Sugiyama 2019

Obligatoria desde mayo de 2018, esta ley ha reforzado el control sobre las prácticas de tratamiento de datos y establece elevadas sanciones a las empresas que la incumplan. El RGPD también amplía la jurisdicción respecto a la legislación anterior, de manera que incluso las empresas extranjeras que procesan datos de residentes de la UE deben cumplirlo.

A pesar de todo, recurrir a la legislación como única medida para combatir el uso indebido de los datos personales plantea ciertas limitaciones:

1 Intervención a posteriori

Las normativas como el RGPD establecen una serie de normas que las empresas deben respetar cuando recopilan y procesan datos. Las empresas deben poder demostrar que cumplen las normas, de lo contrario las autoridades intervienen aplicando sanciones.[25] Este planteamiento a posteriori no garantiza que el uso de los datos respete la privacidad, puesto que la responsabilidad de cumplir las normas recae en la empresa y es el usuario quien debe intervenir si desea recuperar la propiedad de sus datos.

2 Los datos que no tienen carácter personal podrían afectar igualmente a la privacidad

La definición de datos personales es otra de las limitaciones. Difiere en función de la jurisprudencia y de si la normativa sobre recopilación de datos personales puede realmente limitar la práctica de la publicidad dirigida o individualizada. En virtud del actual RGPD, por ejemplo, se pueden elaborar perfiles de usuario mediante el rastreo de la actividad online de los usuarios sin recabar explícitamente ningún dato sobre creencias, orientación sexual, raza u origen étnico.[26] La ambigüedad de la normativa vigente permite a las empresas utilizar variables sustitutivas, características inferidas basadas en los gustos o el comportamiento online del usuario. Con perfiles elaborados a partir de datos no personales, las empresas pueden inferir información personal sensible.

[25] RGPD 2019

[26] Wachter 2019

3 La anonimización de los datos personales no siempre es efectiva

Una de las medidas que promueve y recomienda el RGPD es la anonimización de datos. Según el reglamento, los datos personales dejan de serlo por medio de la anonimización. Sin embargo, algunos estudios recientes revelan la imposibilidad de que los analistas protejan completamente las identidades reales en los conjuntos de datos. En la mayoría de los casos, los datos anonimizados se pueden cruzar con información de otras bases de datos hasta identificar su origen.[27] Esta limitación pone de manifiesto los desafíos y las complejidades de la gobernanza de los datos.

4 Entre la teoría y la práctica

El RGPD ha recibido críticas por su ambigüedad e indefinición respecto a cómo aplicar los distintos artículos.[28] Para algunos expertos, la normativa avanza hacia los principios de la privacidad desde el diseño, pero se queda corta a la hora de ofrecer directrices de cumplimiento concretas a las empresas.[29] Un ejemplo que ilustra esta deficiencia es el consentimiento.

El consentimiento es uno de los métodos más habituales que utilizan las empresas para obtener datos personales, entre otras cosas porque es uno de los requisitos legales más fáciles de cumplir.[30] Aunque el RGPD aclara que el consentimiento debe ser voluntario y que los usuarios deben comprender y aceptar explícitamente la forma en que se utilizarán sus datos, para que se hiciese realidad los formularios de consentimiento deberían emplear un lenguaje sencillo (sin jerga jurídica), dinámico (que permita retirar el consentimiento) y detallado (que ofrezca distintas formas de consentimiento).[31]

La eficacia de los mecanismos de consentimiento es objeto de intenso debate entre los expertos.[32] Aunque los instrumentos de consentimiento se concibieron para permitir a los usuarios tomar decisiones sobre sus datos personales conscientemente, los expertos jurídicos cuestionan su viabilidad y el hecho de que la responsabilidad deba recaer en los usuarios, ya que es difícil que tengan en cuenta todas las posibles ramificaciones al dar el consentimiento.[33]

[27] Ohm 2010

[28] Downes 2019

[29] European Agency for Network and Information Security 2018

[30] GDPR.eu 2019

[31] Ibid.

[32] Herrle and Hirsh 2019

[33] Ibid.

Más allá de la normativa

Estas son sólo algunas de las limitaciones que ilustran las dificultades a las que se enfrentan los responsables políticos para adaptarse al ritmo de las empresas tecnológicas en el contexto de la gobernanza de datos. Aunque la normativa sobre protección de datos puede parecer el único mecanismo para frenar la extracción de datos, los gobiernos tienen otros medios a su alcance para frenar activamente los modelos de monetización de datos personales en la era de la economía basada en datos.

La economista Mariana Mazzucato sostiene que los gobiernos tienen un papel determinante en la creación de mercados, no sólo en su regulación. "No se trata de prescribir tecnologías específicas", explica, "sino de proporcionar directrices de cambio que, desde abajo, permitan experimentar soluciones".[34] En cuanto al emprendimiento, Mazzucato considera que los gobiernos actúan canalizando las oportunidades tecnológicas al crear "una red de actores interesados (no necesariamente actores 'ganadores') dispuestos a aprovechar la oportunidad a través de asociaciones público-privadas".[35]

Privacy-first: un nuevo modelo de negocio digital

En la actual economía de datos, basada en la extracción y la vigilancia, esos "actores interesados" son empresas que responden a la necesidad del mercado de una mayor privacidad de los datos.

Dado que las empresas *privacy-first*, no son las únicas que ofrecen alternativas a la extracción de datos, en la siguiente tabla se muestran otros actores de este ecosistema emergente, así como las ventajas e inconvenientes que implican para los usuarios. La yuxtaposición de estas empresas ofrece una perspectiva más amplia de cómo las empresas que anteponen la privacidad se posicionan en del mercado digital general.

[34] Mazzucato 2015

[35] Mazzucato 2017

Ecosistema de las empresas y herramientas que respetan la privacidad

La siguiente tabla trata sobre diferentes tipos de actores del ecosistema de la privacidad digital. Pueden compartir el mismo objetivo y los mismos retos, pero la principal diferencia es que las empresas *privacy-first* ofrecen una alternativa a una herramienta dominante.

Categoría	Descripción	Ejemplo	Beneficio	Desventaja
Empresas dominantes que protegen la privacidad	El modelo de negocio les permite dar prioridad a la privacidad y la seguridad, ya que los beneficios se obtienen por otros medios, por ejemplo a través de dispositivos de hardware y/o servicios de suscripción.	• Apple.[36]	La fidelidad del usuario es la prioridad; estos negocios buscan garantizar la lealtad del cliente a través de la generación de confianza. Una postura firme sobre la privacidad y la seguridad para garantizar la lealtad del usuario.	• La privacidad no es la fuerza impulsora, es un valor añadido porque los ingresos no dependen de la monetización de los datos. • La privacidad tiene un precio para los usuarios; por ejemplo, los dispositivos de Apple son caros. • Forma parte, indirectamente, del ecosistema de la vigilancia; no promueve activamente un ecosistema más privado.
Herramientas que mejoran la privacidad	Complementos que hacen que las herramientas de uso convencional sean más respetuosas con la privacidad.	• Servicios VPN (TunnelBear, Mullvad, NordVPN), gestores de contraseñas (1Password, LastPass), y bloqueadores de contenido web (NoScript, UBlock Origin).	Los usuarios pueden seguir utilizando las herramientas de uso mayoritario a las que están acostumbrados.	• Añaden responsabilidad al usuario. • Las utilizan sobre todo usuarios. comprometidos con la privacidad. • Tienen un coste, lo que supone un obstáculo de más por su adopción. • Algunos negocios dependen indirectamente del modelo de monetización de datos.
Herramientas que potencian la privacidad	Estas empresas intentan dar poder al usuario ofreciéndole una contrapartida por el uso de sus datos. Estas herramientas tratan de liberalizar el poder de los datos, al mismo tiempo que protegen la privacidad de los usuarios.	• Por ejemplo servicios de datos personales, sin ánimo de lucro y comerciales: Digi.Me, Midata, SoLID, MyDex.	A los usuarios se les da el control de sus datos, y son ellos los que deciden "alquilarlos" a la empresa a cambio de sus servicios. Los usuarios pueden obtener algún beneficio a cambio.	• Pueden crear una nueva brecha entre usuarios que obtienen beneficios por compartir sus datos y otros que no. • La privacidad de los datos de los usuarios no está garantizada; el objetivo principal es distribuir los beneficios de los datos.
Alternativas *Privacy-first*	Estas empresas ofrecen una alternativa más privada o segura a la herramienta de uso convencional y permiten a los usuarios dejar de depender del ecosistema de extracción de datos.	• e-mail: Tor, ProtonMail, Tutanota, Posteo, Mailfence. • Servicios para compartir archivos: NextCloud, Sync. • Búsqueda en la web: DuckDuckGo, Ecosia, Starpage, Brave. • Análisis web: Fathom, Matomo.	Los usuarios pueden usar el producto con la certeza de que su privacidad es el principal interés de la empresa.	• Puede que para usarlos o configurarlos se requiera mayores conocimientos técnicos. • El efecto de red puede restar atractivo a la comodidad. • Tienen un coste, lo que supone una capa más de desacuerdo.

Ilustración 4: ecosistema del respeto a la privacidad

Origen del contenido: Digital Future Society

[36] Etherington 2019

2

Casos prácticos

Las empresas respetuosas con la privacidad buscan sustituir una herramienta de uso convencional por una alternativa que respete la privacidad, ya sea un motor de búsqueda o un gestor de correo electrónico. Las empresas que dan prioridad a la privacidad son únicas porque no hacen recaer la responsabilidad de la protección de datos en el usuario. Están concebidas de tal manera que la protección de los datos sea inherente y operativa desde el principio. Los datos personales que recogen son mínimos y, a diferencia del modelo comercial de extracción de datos, tratan los datos de forma transparente y segura.

Con el fin de responder a la cuestión principal, es decir, cómo los responsables de formulación de políticas pueden apoyar e incentivar modelos que antepongan la privacidad, en el presente informe se analizan cuatro casos prácticos de empresas *privacy-first* rentables: DuckDuckGo, ProtonMail, Nextcloud y Matomo.[37] Estas empresas no sólo cumplen con la normativa vigente, sino que disponen además de otros mecanismos para garantizar la confianza, por ejemplo auditorías, rendición de cuentas y posibilidad de verificación. Todas ellas consideran al usuario el principal beneficiario y comparten una estrategia a largo plazo parecida: construir un Internet más privado.

Y lo más importante: este informe identifica las alternativas existentes para señalar la importancia de los modelos *privacy-first* a la hora de propiciar un cambio del paradigma explotador de la actual economía de datos, sobre todo teniendo en cuenta que los modelos de extracción de datos pueden seguir realizando prácticas invasivas de creación de perfiles y seguimiento del comportamiento incluso dentro del marco regulatorio actual.

[37] Veáse Annexo II de este informe: una lista de negocios *privacy-first*

DuckDuckGo

DuckDuckGo es un motor de búsqueda que no rastrea el comportamiento de los usuarios ni recoge datos personales. Fundado en 2008 por Gabriel Weinberg, DuckDuckGo es una conocida alternativa a los principales motores de búsqueda en lo que respecta a la privacidad. Con una plantilla de 86 personas, su sede está en una pequeña ciudad de los Estados Unidos. DuckDuckGo gestiona actualmente un promedio de 1.300 millones de búsquedas mensuales, habiendo experimentado un crecimiento exponencial en los últimos años.[38] Sin embargo, su cuota de mercado sigue siendo minúscula (0,4%) en comparación con los principales motores de búsqueda.[39]

Misión y visión

Según la empresa, "demasiada gente cree que Internet y privacidad son incompatibles. No estamos de acuerdo, por eso hemos nos hemos propuesto la misión de crear una nueva referencia de confianza online".

Compromiso con la privacidad, la seguridad y la transparencia

DuckDuckGo no nació siendo un buscador que protegía la privacidad. Weinberg pretendía inicialmente perfeccionar la experiencia del usuario al realizar las búsquedas online con mejores resultados, menos desorden y sin spam. Al darse cuenta de la creciente preocupación por la privacidad entre los usuarios, la adoptó como una causa personal, apostando que a largo plazo se convertiría en una preocupación cada vez mayor para los usuarios de Internet.[40]

En cuanto a la propuesta de valor, la principal diferencia entre DuckDuckGo y otros motores de búsqueda es que no comparte los términos de búsqueda con terceros. Aunque recopila palabras clave, no las vincula a usuarios ni identifica a las personas que las han utilizado. A diferencia de la mayoría de los sitios web, DuckDuckGo no almacena datos que identifiquen al usuario, por ejemplo la dirección IP.[41]

Por otro lado, la aplicación móvil y la extensión del navegador ofrecen un sistema de medición de la privacidad (Privacy Grade) que muestra en qué medida se puede confiar en un sitio.[42] Entre sus funciones destacan forzar las conexiones cifradas siempre que sea posible e impedir que los anunciantes rastreen a los usuarios en los sitios que visitan.

La arquitectura de DuckDuckGo se basa en parte en software libre y de código abierto (FOSS, del inglés Free and Open Source Software).[43] Además, la empresa está reforzando su compromiso con el desarrollo de software colaborativo a través de su página GitHub,[44] centrándose en respuestas instantáneas, sitios estáticos y la plataforma social, entre otros.

[38] Lomas 2018
[39] StatCounter 2019
[40] Weinberg 2011
[41] DuckDuckGo 2019
[42] Ibid.
[43] Ibid.
[44] Github 2019

Por último, desde la creación de DuckDuckGo, la empresa ha realizado casi todos los años donaciones a organizaciones que ayudan a mejorar los estándares de confianza online. En 9 años, el volumen total de donaciones ha alcanzado los 1,9 millones de dólares. Esta lucha por reconstruir la confianza en el negocio digital se refuerza a través del blog Spreadprivacy.com, que incluye consejos de privacidad para los usuarios y material educativo para difundir y concienciar sobre la privacidad en la red.

Modelo de negocio

Todas las herramientas de DuckDuckGo (motor de búsqueda, aplicaciones y extensión del navegador) son gratuitas. La empresa genera ingresos de dos maneras. La primera es a través de la publicidad contextual: los anuncios que aparecen en la página de búsqueda se basan en los propios términos de búsqueda, no en otros datos almacenados, como sucede con los principales motores de búsqueda. Los anuncios, distribuidos a través de la red de Yahoo!, aparecen en forma de enlaces patrocinados en la parte superior de la página.

La segunda fuente de ingresos es la asociación con las plataformas de comercio electrónico Amazon y eBay. Si un usuario visita estos sitios a través de DuckDuckGo y realiza una compra, la empresa recibe una pequeña comisión.

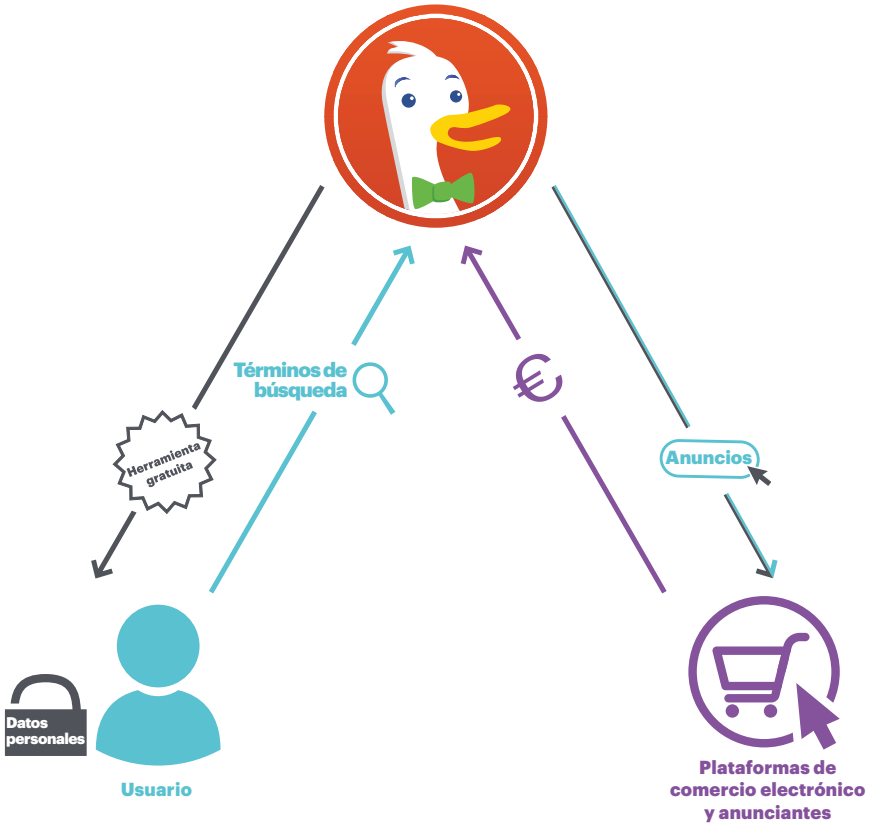


Ilustración 5: modelo de negocio de DuckDuckGo

Origen de la Imagen: adaptada de Business Model Toolbox

Fuente: DuckDuckGo 2019

Financiación

DuckDuckGo no es el primer proyecto de Weinberg. Después de graduarse en el MIT, Weinberg creó una empresa de software educativo.[45] Más tarde lanzó Names Database, una red social que fue adquirida por Classmates.com en 2006 por 10 millones de dólares.[46]

DuckDuckGo se autofinanció hasta 2011. En ese año, Union Square Ventures inyectó 3 millones de dólares al proyecto, y en 2018 la rama de capital de riesgo del fondo de pensiones canadiense Omers invirtió otros 10 millones de dólares.[47]

Pocos años después de crearse, la empresa ya había experimentado un crecimiento significativo. En 2012, DuckDuckGo ya había conseguido una media de 1,5 millones de búsquedas al día. En 2014, Apple lo incluyó entre los motores de búsqueda predeterminados disponibles del navegador Safari, y Mozilla hizo lo propio con Firefox. En 2019, incluso su competidor directo, Google, empezó a añadir DuckDuckGo a la lista de posibles motores de búsqueda de Chrome. En noviembre de 2019, DuckDuckGo alcanzó una cifra récord de búsquedas en un sólo día: 50,9 millones.

Principales aportaciones

- DuckDuckGo demuestra que un motor de búsqueda gratuito es capaz de generar ingresos sin necesidad de extraer datos de los usuarios y con publicidad contextualizada, una alternativa no invasiva.
- La estrategia a largo plazo de DuckDuckGo va en línea con los valores de la empresa y también con el mercado. El desarrollo de otras herramientas de protección de la privacidad es un indicador que señala su acierto al apostar por el crecimiento sostenible.
- El fundador de la empresa, Weinberg, es un emprendedor nato cuya experiencia previa en la obtención de capital le dio una ventaja a la hora de presentar DuckDuckGo a las empresas de capital riesgo, que apostaron por la trayectoria de Weinberg.[48]
- Aunque el punto fuerte de la empresa es la privacidad, también se esfuerza por ofrecer una mejor experiencia de usuario con búsquedas precisas, ordenadas y poco spam.
- La defensa de la privacidad de DuckDuckGo destaca la interdependencia de los modelos empresariales que anteponen la privacidad y la necesidad de que exista un ecosistema basado en el respeto a la privacidad que ofrezca a los usuarios un Internet de confianza donde los datos personales estén seguros.

[45] Chan 2019

[46] Sec.gov 2006

[47] Lomas 2018

[48] Burnham 2011

ProtonMail

Andy Yen, Jason Stockman y Wei Sun crearon ProtonMail en 2014, en las instalaciones del Organización Europea de Investigación Nuclear (CERN). El objetivo principal de ProtonMail, que cuenta con más de 10 millones de usuarios, es proteger y garantizar la seguridad de los datos de los usuarios a través de correo electrónico encriptado. Es una respuesta al modelo de negocio basado en la extracción de datos y los ingresos publicitarios y busca transformar los servicios de correo electrónico al ofrecer uno que priorice la protección de los datos. En 2018, ProtonMail se asoció con Mozilla para desarrollar Proton VPN, un servicio de red privada virtual seguro y gratuito que tiene más de 1 millón de usuarios.

Misión y visión

"Estamos construyendo un Internet que protege la privacidad, empezando por el correo electrónico".

El equipo de ProtonMail afirma compartir la visión y el reto de "proteger los derechos de la sociedad en Internet". Para conseguirlo se ha marcado el objetivo de crear una herramienta de correo electrónico accesible y fácil de usar destinada al mayor número de personas posible.[49] A largo plazo, la empresa busca desarrollar herramientas de privacidad complementarias que amplíen el acceso a sus servicios y también expandir el paquete de productos ProtonMail para que incluya un calendario, un servicio de almacenamiento y un editor de documentos.

Compromiso con la privacidad, la seguridad y la transparencia

ProtonMail garantiza la privacidad encriptando los mensajes en el navegador web del usuario antes de que lleguen a los servidores de ProtonMail. En el ordenador del usuario se genera una doble clave, y dado que ProtonMail no tiene ni la contraseña ni las claves de descifrado, no pueden acceder a los mensajes del usuario.

Además de asegurar la encriptación de extremo a extremo, el servicio de correo no registra las direcciones IP de los usuarios ni almacena los datos encriptados de los usuarios en la nube. Utiliza un servidor administrado en Suiza (en un búnker situado a mil metros bajo los Alpes suizos). Los creadores eligieron Suiza porque cuenta con las leyes de privacidad más estrictas del mundo y permanece fuera de las jurisdicciones de EE.UU. y la UE.

ProtonMail empezó a hacer públicas poco a poco algunas partes de sus paquetes de software y tiene previsto seguir haciéndolo a medida que crezca. Que el código y la encriptación sean accesibles y puedan inspeccionarse refuerza la transparencia y la capacidad de supervisión.[50]

[49] ProtonMail 2019

[50] ProtonMail 2015

El compromiso de ProtonMail con la transparencia va más allá del software, ya que los estatutos de la empresa, los empleados y la financiación están a disposición del público. Aunque su comunicación es transparente y demostrable en pruebas, su trabajo se somete a verificación por parte de terceros a través de auditorías externas de seguridad y revisiones de expertos, que también se publican.

Parte de la estrategia de comunicación de ProtonMail consiste en desempeñar un papel activo en la sensibilización y la defensa de los derechos de privacidad. Por ejemplo, ha creado GDPR.eu, un recurso para pequeñas empresas que ayuda a cumplir el RGPD, ha intervenido en una conferencia de las Naciones Unidas sobre cómo luchar contra el terrorismo y a la vez proteger los derechos humanos, ha colaborado con Reporteros sin Fronteras y se ha opuesto públicamente a la vigilancia basada en la tecnología de reconocimiento facial no regulada.[51]

Modelo de negocio

La empresa afirma que no muestra anuncios ni gana dinero aprovechándose de la privacidad de los usuarios.[52] Los precios de ProtonMail siguen un modelo gradual. Su servicio gratuito ofrece 500 MB de almacenamiento con un límite de 150 mensajes por día. Si los usuarios desean más almacenamiento, direcciones de correo electrónico, mensajes y asistencia pueden optar por tres paquetes distintos que ofrecen más funciones. Los ingresos de ProtonMail sirven para mantener todas las cuentas (incluidas las de los suscriptores gratuitos), además del servicio de asistencia, la investigación y el desarrollo.

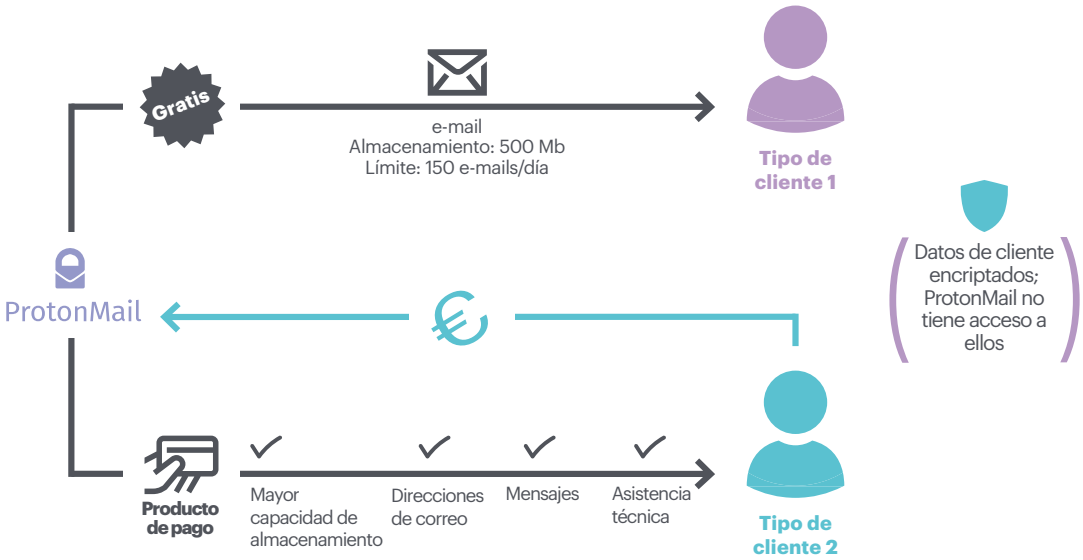


Ilustración 6: modelo de negocio de ProtonMail

Origen de la imagen: adaptada de Business Model Toolbox

Fuente: ProtonMail 2019

[51] ProtonMail 2015

[52] Ibid.

Financiación

ProtonMail comenzó con una campaña de financiación colectiva en Indiegogo en 2014 y recaudó 500.000 euros. Los principales accionistas son personas concienciadas con la privacidad. Dado su compromiso de proteger la privacidad de los usuarios, la empresa se negó inicialmente a aceptar financiación de inversores.[53] Yen, su creador, afirmó en 2014 que "la razón por la que debemos arrancar solos es porque si aceptamos el dinero de algo como Google Ventures, se acabó nuestra credibilidad. Al estar en este mercado tenemos que financiarnos nosotros mismos".[54]

El principal obstáculo con el que se topó ProtonMail fue encontrar financiación privada que se amoldara a los valores de la empresa.[55] En 2015, recibieron 2 millones de dólares de la empresa estadounidense CRV (inversores iniciales de Twitter, Zendesk y Yammer) y la Fondation Genevoise pour l'Innovation Technologique (FONGIT), una fundación sin ánimo de lucro respaldada por el gobierno suizo.[56] A principios de 2019, ProtonMail obtuvo 2 millones de euros del programa Horizonte 2020 de la Comisión Europea para continuar con el desarrollo del ecosistema de Proton. Según la empresa, esta alianza no sólo significa "recibir una importante financiación, sino también contar con un poderoso aliado en las duras batallas que están por venir".[57]

Principales aportaciones

- Para demostrar que un modelo de negocio no se basa en la extracción de datos, la comunicación es clave. ProtonMail es transparente y minuciosa a la hora de explicar cómo protege los datos de los usuarios.
- El centro de investigación del CERN y la propia comunidad desempeñaron un papel destacado en la creación de ProtonMail; la comunidad aportó conocimientos técnicos y probó y validó el producto.
- La legislación suiza en materia de privacidad y el apoyo institucional crearon un entorno propicio para el desarrollo de un servicio de correo que antepone la privacidad.
- Encontrar los socios inversores adecuados fue clave para que ProtonMail se mantuviera firme en sus valores.
- Al coincidir con los intereses de instituciones europeas como FONGIT y Horizonte 2020, ProtonMail consiguió financiación con la que desarrollar nuevas aplicaciones centradas en la privacidad.
- Tener un modelo de precios escalonado puede ser una alternativa útil (entre el enfoque *freemium* y el modelo de suscripción completa) para ampliar la base de clientes y generar al mismo tiempo ingresos suficientes para garantizar la sostenibilidad económica.

[53] ProtonMail 2019
[54] Slade 2014
[55] Ibid.
[56] Sawers 2018
[57] Yen 2015

Nextcloud

Nextcloud es un conjunto de servicios de código abierto creado por Frank Karlitschek y un equipo de ingenieros que ofrece un modelo alternativo a los servicios en la nube centralizados. Karlitschek puso en marcha el proyecto en 2016 después de abandonar OwnCloud, la empresa que había fundado, por diferencias en la estrategia.[58]

El software Nextcloud permite a los usuarios y a las empresas alojar y gestionar sus datos por sí mismos. Además de almacenamiento, Nextcloud permite:

- Sincronizar y compartir, lo que da a los usuarios acceso a los archivos y les permite trabajar con los documentos y compartirlos con el resto del equipo.
- Una plataforma de mensajería que permite a los equipos compartir pantallas o mantener reuniones, con todos los datos almacenados de forma local en el servidor.
- Software colaborativo: su *groupware* integra funciones de productividad, entre ellas calendario, contactos y correo electrónico.

Nextcloud estima que tiene alrededor de 25 millones de usuarios en 300.000 servidores.[59]

Misión y visión

"Desarrollamos software que descentraliza y democratiza los servicios en la nube y ofrece alternativa a los servicios en la nube centralizados".

Nextcloud permite al usuario controlar sus datos al utilizar las herramientas. Espera poderse integrar, a largo plazo, en un ecosistema basado en la privacidad en el que diversos servicios en la nube sean alternativas viables a las soluciones centralizadas y patentadas.

Compromiso con la privacidad, la seguridad y la transparencia

El *software* de Nextcloud está diseñado para que los clientes puedan desarrollar un servicio que se ejecute en su propio servidor o dispositivo. Permite a los usuarios controlar totalmente el almacenamiento de datos y puede integrarse con las herramientas de seguimiento y registro que utilice la empresa. Es compatible con algunos de los mecanismos y protocolos de autenticación más utilizados del mercado.[60]

El propio servicio Nextcloud cumple con los requisitos de privacidad y protección de datos, ya que no recoge ninguna información de los usuarios ni accede a ella. Además, han diseñado el producto de manera que los clientes puedan cumplir fácilmente con el RGPD.

[58] Karlitscheck 2016

[59] Ibid.

[60] Poortvilet 2019

Privacidad y transparencia son los valores primordiales del producto. El autoalojamiento garantiza el control total de los datos, pero Nextcloud también es un software de código abierto, lo que significa que cualquiera puede verificar que no existen "puertas traseras". No hay ningún tipo de atadura al proveedor, puesto que los usuarios pueden ejecutar el software independientemente de Nextcloud con otros proveedores de servicios. Nextcloud es un proyecto de código abierto que cuenta con una gran comunidad de voluntarios; más de 2.000 personas contribuyen añadiendo código al proyecto.

Modelo de negocio

La empresa se fundamenta en un modelo de negocio de código abierto.[61] Nextcloud ofrece una versión gratuita con prestaciones complementarias según las necesidades de los clientes. Si los clientes no tienen los conocimientos técnicos o los recursos necesarios para ejecutar el software, pueden suscribirse y recibir soporte técnico de Nextcloud. Entre las funciones adicionales destacan la asistencia, un servicio de consultoría e integración con Outlook o la suite ofimática de código abierto de Collabora.

La estrategia de crecimiento de Nextcloud se basa en el crecimiento lento, sostenible y orgánico. La empresa, que actualmente tiene 50 empleados, empezó a ser rentable en 2017. Los clientes van desde particulares hasta pymes y grandes empresas, pasando por terceros que gestionan servicios en la nube y ofrecen la posibilidad de usar Nextcloud. Entre los clientes más destacados se encuentran los gobiernos nacionales francés y alemán.

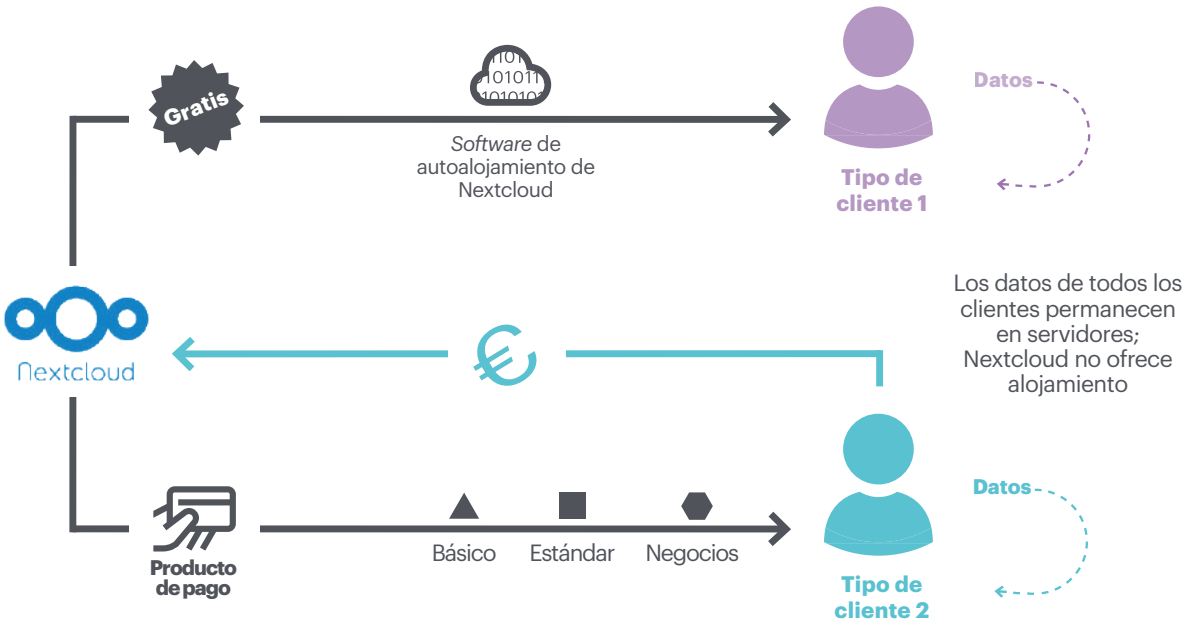


Ilustración 7: modelo de negocio de Nextcloud

Origen de la imagen: adaptada de Business Model Toolbox

Fuente: Nextcloud 2019

[61] Poortvliet 2016

Financiación

Los inversores de Nextcloud son los propios empleados. El fundador, Frank Karlitschek, rehuyó el capital riesgo ya que su anterior empresa, Owncloud, fue sometida a una serie de condiciones que se oponían a su visión de empresa, orientada en el valor.[62]

Principales aportaciones

- Nextcloud ofrece una solución tanto a los particulares como a las empresas que buscan ser propietarios de sus datos.
- Los gobiernos y las empresas a quienes preocupa la creciente concentración y centralización de los datos han mostrado interés por las soluciones empresariales que ofrece Nextcloud.
- Nextcloud es interoperable, lo que significa que los usuarios pueden integrarlo fácilmente en otros sistemas, a diferencia de las herramientas patentadas de la competencia.
- La comunidad es una parte importante del modelo de negocio de Nextcloud, ya que los ingenieros de código abierto contribuyen al código y los empleados a financiar la empresa.
- El modelo empresarial de código abierto promueve la transparencia y la innovación, pero también requiere un esfuerzo adicional por parte de la dirección para mantener el delicado equilibrio de todas las partes interesadas.

[62] Bhartiya 2016

Matomo (Innocraft)

Matomo es una herramienta de análisis web de código abierto que permite a las empresas recabar datos a través de su página web con el fin de tomar decisiones. La empresa que se haya detrás es Innocraft. El software Matomo tiene su origen en Piwik, desarrollado por Matthieu Aubry en 2007 para responder a la necesidad de disponer de una alternativa respetuosa con la privacidad frente a Google Analytics. Se utiliza en más de 200 países y en un millón de sitios web.[63]

Misión y visión

Innocraft pretende convertir Matomo en la plataforma de análisis de código abierto número uno. Su objetivo es formar parte de un movimiento a gran escala que descentralice Internet.

Compromiso con la privacidad, la seguridad y la transparencia

El objetivo de Innocraft es dar a las personas y las empresas el poder de controlar sus datos. La mayoría de los usuarios alojan sus datos analíticos en servidores propios, por lo que Innocraft no puede acceder a los datos de los clientes, lo que consolida el enfoque de privacidad desde el diseño de Matomo. Además, la empresa otorga a los propietarios de los sitios web más control sobre los datos que desean rastrear, lo que les ayuda a cumplir el reglamento RGPD y a garantizar que el comportamiento de los visitantes no se comparta con empresas anunciantes. Anonimiza automáticamente las IP de los visitantes y elimina los registros antiguos de los visitantes.[64]

La empresa pide ayuda a la comunidad de usuarios para detectar problemas de seguridad en el software.[65] También recompensa a quienes encuentren errores de seguridad importantes y aconseja a los usuarios que deseen mejorar la seguridad de su software.

[63] Matomo 2019

[64] Ibid.

[65] Ibid.

Modelo de negocio

Innocraft tiene un modelo de negocio basado en el código abierto. Los usuarios pueden alojar Matomo Analytics en sus servidores y pagar para recibir asistencia o servicios adicionales. Si los clientes no tienen ningún conocimiento técnico, tienen la opción de pagar por almacenar sus datos en la nube. Innocraft también proporciona servicios de alojamiento en la nube a las empresas a través de planes mensuales y anuales. Ofrece tres paquetes distintos que se adaptan a las necesidades de datos, número de sitios web y otras herramientas analíticas. La mayoría de los usuarios están en Europa y los EE.UU.

A pesar de la intención de Innocraft de convertirse en una empresa sostenible, se plantea la duda de si la privacidad y la seguridad son argumentos de venta suficientes para sostener la empresa a largo plazo. Por este motivo la empresa busca desarrollar otras propuestas de valor que vayan en la línea de sus valores fundamentales.

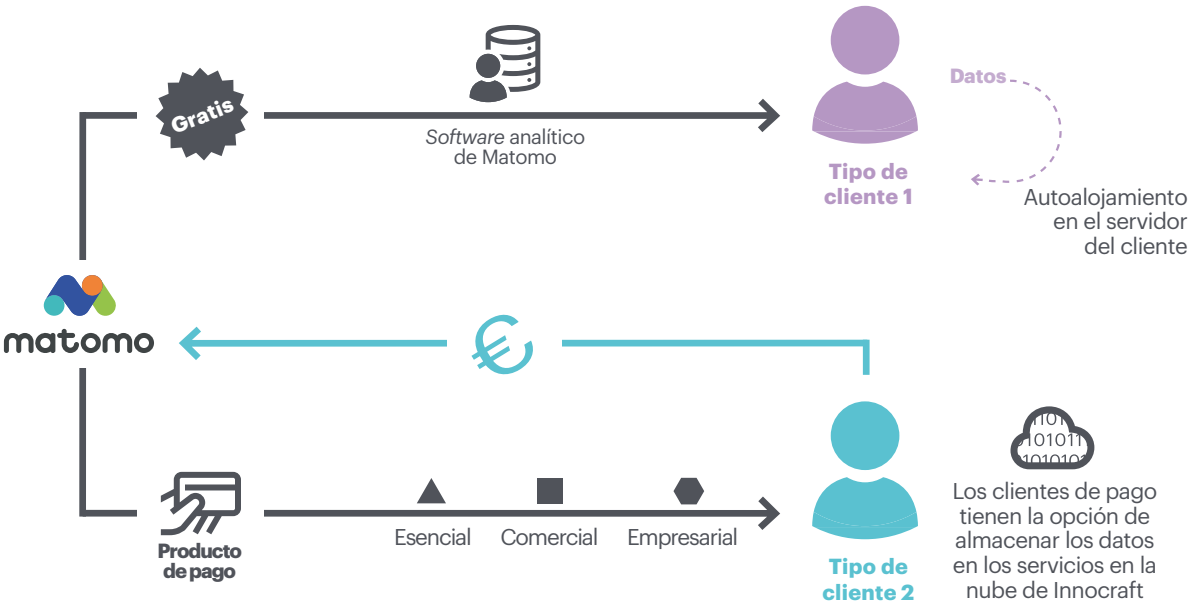


Ilustración 7: modelo de negocio de Innocraft

Origen de la imagen: adaptada de Business Model Toolbox

Fuente: Innocraft 2019

Financiación

Matomo empezó con otro nombre, Piwik, y fue un proyecto financiado por la empresa londinense OpenX,[66] que en aquel momento seguía una estrategia muy centrada en el código abierto. OpenX estaba creando un servidor de publicidad de código abierto y apostó por el proyecto de analítica web de Aubry. Después de poner en marcha el proyecto en 2007 y de que Piwik siguiera desarrollándolo más tarde, finalmente buscaron financiación externa para poder mantenerlo.

Cuando Aubry dejó Piwik y creó Matomo, lo hizo a través de Innocraft. Se trata de una empresa autofinanciada, con sede en Nueva Zelanda, que rápidamente pasó a ser rentable gracias a un pequeño equipo y a un proyecto de código abierto que sólo comercializaba las funciones de empresa. Aubry evitó recurrir a inversores como había hecho anteriormente en Piwik; quería evitar que trataran de controlar el proyecto de código abierto.

Principales aportaciones

- Matomo es una alternativa a Google Analytics. El marketing y los análisis han ido evolucionando hasta abarcar todos los modelos de extracción de datos. Matomo ofrece a las empresas soluciones analizar el funcionamiento del sitio web y a la vez cumplir el RGPD.
- Matomo apoya la descentralización al permitir a las personas y las empresas controlar los datos que rastrean.
- Contar con una comunidad de usuarios fieles es esencial para el éxito de los proyectos de código abierto; Matomo confía en su comunidad para, por ejemplo, resolver los problemas de seguridad.
- La flexibilidad de un producto permite a los usuarios adaptarse a los diferentes perfiles de cliente en función de sus conocimientos técnicos. Matomo puede utilizarse localmente de manera autónoma, pero también proporciona apoyo técnico especializado a quienes lo necesitan.
- Esta flexibilidad también tiene en cuenta la envergadura de cada cliente y sus necesidades, ya se trate de pymes o de gigantes tecnológicos.

[66] OpenX 2019

3

Desafíos y oportunidades

Obstáculos a los que se enfrentan los modelos de negocio *privacy-first*

Las empresas presentadas en los anteriores casos prácticos demuestran que es posible tener éxito con un modelo de negocio que anteponga la privacidad del usuario. Todas ellas comparten el objetivo común de sensibilizar sobre los modelos empresariales de explotación que proliferan en la economía de los datos, y su estrategia a largo plazo consiste en crear confianza en un ecosistema digital reinventado el tratamiento de los datos de forma privada y transparente. La actual cultura de monetización de datos crea un entorno lleno de obstáculos para los modelos comerciales alternativos, que se enfrentan a desafíos variados e interrelacionados.

Encontrar la financiación adecuada

La financiación es una de las principales inquietudes de cualquier nueva empresa. La vía más habitual a la que recurren las empresas digitales de nueva creación es el capital de riesgo, aunque este tipo de inversores sólo suelen apoyar aquellas empresas que tienen la capacidad de generar beneficios o crecer rápidamente. Los modelos empresariales *privacy-first*, sin embargo, no se basan en la monetización de los datos, por lo que el crecimiento exponencial no es tan sencillo.

Los cuatro casos estudiados ilustran la variabilidad y la complejidad del acceso a la financiación. DuckDuckGo se autofinanció inicialmente y luego recibió el respaldo de inversores de capital de riesgo. El equipo fundador de Nextcloud también autofinanció la empresa, mientras que ProtonMail se benefició del apoyo de una comunidad volcada en la privacidad que financió en proyecto de manera participativa, con la posterior inyección de capital de riesgo y financiación pública. Matomo, antes Piwik, fue incubada inicialmente por una empresa de éxito, superó rondas de financiación, y después pasó a ser autofinanciada por sus propios empleados.

Dada la cultura de la financiación de capital riesgo, las empresas centradas en valores deben buscar más allá de las vías tradicionales de inversión, lo que incluye explotar otras fuentes de capital como la inversión de impacto social o la financiación colectiva. Si finalmente optan por la financiación de capital de riesgo, los empresarios *privacy-first* deben conocer los términos y condiciones del acuerdo y las consecuencias para su empresa. Con todo, no existe una solución universal y preceptiva. ProtonMail y DuckDuckGo demuestran que la financiación de capital riesgo también es una vía posible siempre que los valores y objetivos de la empresa y los de los inversores coincidan.

Esperanza de vida

Los anteriores casos prácticos muestran cómo las empresas *privacy-first* priorizan los valores y suelen experimentar una disyuntiva entre la fidelidad a los valores y la generación de beneficios. Por ejemplo, Matomo y Nextcloud se enfrentaron a luchas internas y a estrategias empresariales en conflicto. La presión a la que se enfrentan Matomo y Nextcloud es doble: no sólo dan prioridad a la privacidad, sino que ambas se basan en un modelo de negocio de código abierto.

Los modelos comerciales basados en el código abierto consideran a la comunidad de desarrolladores tanto clientes como colaboradores esenciales que construyen, utilizan y mejoran el *software* de manera participativa. En estos modelos, la confianza entre la dirección y la comunidad es crucial para crear un producto sostenible. Jos Poortvliet, director de marketing de Nextcloud, subraya que ganar dinero e ir más allá del trabajo de los voluntarios y las donaciones es un gran desafío para que los modelos de negocio de código abierto sean sostenibles.

El compromiso con la comunidad es algo que las empresas *privacy-first* no están dispuestas a poner en riesgo aunque a veces pueda ser una carga. Por el contrario, los competidores que explotan datos ven en la confianza algo secundario y sí pueden permitírselo, ya que su producto genera ingresos a pesar de la falta de confianza. Dado que la confianza es el núcleo de su propuesta de valor, las empresas que anteponen la privacidad deben tomar decisiones difíciles que pueden pasar por renunciar a los beneficios. En palabras del director general de ProtonMail, Andrew Yen:

> **"La mayor parte de este trabajo crítico [crear una infraestructura fiable y segura] se realiza entre bastidores, pero en cuestión de prioridad, siempre se antepone a las nuevas funciones. Aunque todo el mundo esté impaciente, como es comprensible, por disfrutar de nuevas funciones (nosotros también), si las cosas llevan más tiempo del esperado suele ser porque estamos invirtiendo en crear una infraestructura aún más importante y en medidas contra el abuso".[67]**

Las empresas *privacy-first* crecen lentamente, lo que también las coloca en una posición vulnerable y las convierte en blanco fácil de comportamientos anticompetitivos. Según ProtonMail, Google ocultó intencionadamente a ProtonMail en los resultados de búsqueda durante 10 meses, lo que provocó que el índice de crecimiento disminuyera un 25% en todo el mundo. Entre 2010 y 2018, Google también fue propietario de la URL duck.com, que redirigía a los usuarios a la búsqueda de Google. Sólo cedió duck.com a DuckDuckGo cuando este se quejó públicamente en las redes sociales de que Google estaba confundiendo a los usuarios a propósito.

[67] Yen 2018

La dificultad de captar nuevos usuarios

Las empresas con modelos de negocio basados en la extracción de datos son especialmente atractivas para los inversores porque el valor de su producto aumenta a medida que su base de usuarios crece. La mayoría de plataformas de éxito se benefician en su modelo de negocio de los efectos de red. En vez de eso, las empresas orientadas a la privacidad tienen que buscar estrategias de crecimiento alternativas que vayan más allá de los nichos de mercado y la cultura "de lo gratuito".

En los cuatro casos estudiados, las empresas ofrecen parte (o la totalidad, en el caso de DuckDuckGo) de sus productos o servicios de forma gratuita y rentabilizan las funciones adicionales o el soporte técnico. La mayor dificultad a la hora de captar nuevos usuarios limita el efecto de red, tan importante para las alternativas gratuitas. En los últimos años, numerosos proyectos que ofrecían alternativas basadas en la privacidad han fracasado por esta razón, ya que no lograron llegar a un número significativo de usuarios que les permitiera competir con los líderes del mercado.[68]

Para conservar a los usuarios, las empresas *privacy-first* también deben ofrecer un servicio que sea tan bueno o mejor que el que domina en el mercado. Como explica el fundador de Nextcloud, Frank Karlitschek, "debes ofrecer todas las funcionalidades que el usuario espera", ya que si el servicio no tiene todas las funciones esperadas, el usuario volverá a las herramientas de uso convencional o se buscará otro servicio.[69]

Oportunidades para las empresas *privacy-first*

Aunque las empresas que dan prioridad a la privacidad se enfrentan a muchos desafíos, los proyectos con un enfoque ético de la privacidad y los datos cada vez suscitan mayor interés.

Responder a la inquietud social sobre la privacidad

Las empresas que basan su actividad en los datos han sufrido numerosos problemas de seguridad y violaciones de datos en los últimos años. Los fallos de seguridad son una oportunidad que los modelos de negocio centrados en la privacidad pueden aprovechar.

ProtonMail es un servicio de mensajería cifrada alternativo a Gmail, el correo electrónico más utilizado del mundo y objeto de diversos ataques que han puesto en jaque la información de millones de usuarios.[70] Nextcloud, que ofrece alojamiento propio, es una alternativa a los sistemas de almacenamiento en la nube dominantes como Dropbox, víctima de varios

[68] Newman 2018

[69] Mozilla 2019

[70] Johnson 2017

ciberataques que filtraron las contraseñas de los usuarios. Matomo, por su parte, es una alternativa a Google Analytics, una herramienta cada vez más cuestionada por las empresas que anteponen la privacidad.[71]

Los negocios centrados en la privacidad podrían ganar popularidad en los próximos años, sobre todo porque las generaciones jóvenes son más conscientes de la importancia de la privacidad que las que las preceden.[72] También los gobiernos muestran mayor interés por las herramientas que fomentan la privacidad. Aunque algunos siguen utilizando herramientas de gestión desarrolladas por grandes empresas,[73] cada vez hay más países que exigen alternativas que garanticen la confidencialidad y la seguridad de los datos.

Un sector tecnológico cambiante

El desarrollo de tecnologías más éticas es una tendencia que está tomando fuerza en la nueva generación de empresas emergentes.[74] Así lo entendió la empresa de inversión Union Square Ventures cuando decidió reunirse con DuckDuckGo en 2011. "Invertimos en DuckDuckGo porque nos convencimos de que no sólo es posible un cambio de paradigma en los motores de búsqueda, sino que había llegado la hora de propiciarlo", asegura Brad Burnham, socio de USV.[75]

El movimiento Zebras Unite,[76] una organización que fomenta una cultura de *startup* más ética e inclusiva, ilustra bien ese distinto enfoque de negocio. Las cebras, a diferencia de los unicornios, son empresas que dan prioridad al crecimiento sostenible frente al exponencial y al interés del público por encima del dominio del mercado.

Otra tendencia al alza en el sector tecnológico es la expansión del código abierto, cada vez más utilizado para desarrollar y compartir soluciones tecnológicas.[77] Este movimiento, que persigue que la tecnología esté al alcance de todos y adopta principios como el de la transparencia, se propaga por las administraciones y las organizaciones internacionales, por ejemplo las Naciones Unidas a través los Laboratorios de Innovación Tecnológica de las Naciones Unidas (UNTIL).[78]

La necesidad de soluciones concretas

Las empresas que anteponen la privacidad podrían tener cierta ventaja en sectores en los que la confidencialidad de los datos y la seguridad son prioritarias. El sector sanitario y el jurídico, por ejemplo, tratan información confidencial sensible y podrían beneficiarse de soluciones que protejan los datos tanto del usuario como del propio sector, que por otra parte presenta numerosas oportunidades de negocio. El proyecto de aprendizaje automático de Google, cuyo nombre en clave es Nightingale, es un ejemplo que muestra la importancia

[71] Schwab 2019
[72] Raicu 2016
[73] Infobae 2016
[74] Montgomery 2019
[75] Burnham 2019
[76] Zebras Unite 2019
[77] Volpi 2019
[78] UNTIL 2019

de las soluciones basadas en la privacidad. Una investigación de 2019 reveló que no sólo no se informó a los médicos y a los pacientes sobre el uso de datos de pacientes, sino que 150 empleados de Google tuvieron acceso a información sanitaria confidencial.[79]

Las empresas que anteponen la privacidad la sitúan en el centro de su modelo de negocio, por lo que parten de un planteamiento que haría más fácil no caer en semejantes errores garrafales. ProtonMail, por ejemplo, reconoce la naturaleza confidencial del correo que intercambian determinadas profesiones y destinatarios y centra el marketing y la comunicación en periodistas, activistas, funcionarios, entidades sin ánimo de lucro, etc.[80]

También los gobiernos muestran cada vez mayor interés por controlar al máximo la seguridad de la información y están tomando medidas para crear infraestructuras nacionales de datos. Como se vio en el apartado anterior, Nextcloud ha dado respuesta a las necesidades de control interno de datos de los gobiernos de Francia y Alemania.[81] La administración gala también ha sustituido a Google por el motor de búsqueda local y centrado en la privacidad Qwant.[82]

La legislación vigente en materia de protección de datos de la UE reclama soluciones concretas a la centralización de los datos. El Supervisor Europeo de Protección de Datos exige a las instituciones y los gobiernos europeos que controlen los datos y conozcan su finalidad y paradero, aunque los procesen terceros. Este requisito ha puesto en entredicho los contratos de la UE con proveedores como Microsoft y ha allanado el camino a las empresas centradas en la privacidad.[83]

[79] Fussell 2019

[80] Wolford 2019

[81] Nextcloud 2019

[82] Goujard 2018

[83] Lomas 2019

4

Pasar a la acción

Incentivos para modelos de negocio *privacy-first*

Como hemos visto, las empresas *privacy-first* se enfrentan a muchos desafíos, el principal de ellos su excepcionalidad dentro de la industria tecnológica. Deben hacer frente a poderosos competidores que se aprovechan de los efectos de red y de herramientas patentadas, por lo que tienen dificultades para acceder a la financiación y para convertirse en empresas sostenibles.

Sin embargo, cada vez surgen más oportunidades en el mercado para empresas que anteponen la privacidad. El número de empresas, gobiernos y ciudadanos que toman conciencia de la importancia de la transparencia y la privacidad en el uso que las empresas tecnológicas dan a sus datos va en aumento.

Para aprovechar las oportunidades que se presentan en la sección 3, los responsables políticos deben actuar. El presente informe concluye con tres iniciativas que los gobiernos pueden poner en práctica para incentivar las empresas *privacy-first*. Se trata de iniciativas concebidas por el grupo de trabajo y que responden a los retos concretos a los que se enfrentan estas empresas.

Iniciativa 1: certificación de empresas *privacy-first*

QUÉ

Crear un instrumento con el que evaluar y certificar las empresas *privacy-first* aumentaría la concienciación sobre los modelos comerciales alternativos y fomentaría la confianza de los consumidores al desenmascarar las iniciativas que sólo apuestan por la privacidad de cara a la galería. Establecer una certificación basada en el modelo de certificaciones existentes (como la de B-Corp[84]) podría atraer el apoyo de gobiernos, consumidores y otras empresas.

POR QUÉ

Como se ha explicado en la sección anterior, los parámetros diseñados para medir el éxito potencial de una empresa favorecen a un tipo de empresa: la que da prioridad al crecimiento exponencial frente al crecimiento sostenible. Los modelos de empresas que se fundamentan en una propuesta de valor están en desventaja, ya que no existe una fórmula que permita medir su éxito.

Así pues, urge crear nuevos parámetros que midan el éxito empresarial más allá de los beneficios o del número de usuarios. La certificación propuesta analizaría indicadores como la sostenibilidad, la transparencia y la protección del derecho a la privacidad de los usuarios, lo que haría que los responsables políticos estuvieran más predispuestos a contratar empresas que respetan la privacidad.

Contar con una certificación única no sólo beneficiaría a la compra pública. Como señala la consultora Edelman, "las marcas se están viendo obligadas a ir más allá de los clásicos intereses comerciales para convertirse en defensoras de una sociedad mejor".[85] Ya existen varios proyectos que analizan el "respeto a la privacidad" de las empresas tecnológicas, como "That one privacy site"[86] o PrivacySpy.[87] Aunque estas iniciativas ayudan a sensibilizar a los consumidores sobre la importancia de la privacidad de los productos y servicios digitales, su difusión es limitada y aún no se han generalizado.

[84] Bcorporation.net 2019

[85] Edelman 2019

[86] Thatoneprivacysite.net 2019

[87] PrivacySpy 2019

CÓMO

La creación de un certificado centrado en la privacidad requiere establecer una lista de criterios que los solicitantes deben cumplir, además de una entidad se encargue de la acreditación, la supervisión y la auditoría de empresas.

Las cada vez más numerosas iniciativas públicas dirigidas a supervisar cómo la tecnología basada en datos afecta a la sociedad son un ejemplo que podría aplicarse a la certificación. El Centro de Ética e Innovación de Datos del Reino Unido y el Consejo de Ética de Datos de Dinamarca son dos iniciativas públicas que reúnen a expertos de diversos sectores y asesoran a los responsables políticos en materia de gobernanza tecnológica. Estas entidades auspiciadas por el gobierno podrían servir de modelo para una secretaría que promueva y gestione una certificación que premie la privacidad.

La función de supervisión podría recaer posteriormente en una entidad regional o global que garantizara el cumplimiento de los criterios de certificación acordados. Esta entidad certificaría a su vez a organismos de acreditación independientes que se encargarían de evaluar si una empresa cumple los criterios establecidos. El cometido de la secretaría sería supervisar a esos organismos de certificación independientes y asegurarse de que cumplen las normas. Para garantizar la rendición de cuentas y la transparencia, la secretaría debería estar bajo la supervisión de:

- Una junta de expertos que acuerde los criterios de concesión de la certificación.
- Dos comités consultivos: uno compuesto por ciudadanos y otro por representantes del gobierno.
- Un auditor que evalúe de manera independiente si los organismos de acreditación cumplen las normas establecidas por la secretaría.

Al crear esta estructura de gobierno es importante prever posibles conflictos de intereses entre los miembros destinados a formar parte de la secretaría. Además, los responsables políticos deben tener presente la necesidad de elegir partes interesadas heterogéneas que representen a todo el sector empresarial digital.

Una vez establecida la estructura autorregulada, la junta de expertos debe establecer un conjunto de normas de certificación con las que evaluar si el modelo comercial se basa en la monetización de datos y si su actividad contribuye a fomentar la competencia. Además, la junta debería fijar y hacer público el proceso de certificación con claridad y determinar la frecuencia de las auditorías.

Iniciativa 2: contratar a empresas *privacy-first*

QUÉ

El sector público puede influir directamente en los mercados digitales dando ejemplo. Una forma de hacerlo es aprovechar las licitaciones públicas para contratar empresas que traten los datos de los usuarios de manera responsable.

Para incluir un requisito concreto en los procesos de contratación pública es necesario establecer criterios y someterlos a pruebas graduales en cada sector. Por ejemplo, la iniciativa podría ponerse a prueba en dos áreas muy específicas de los servicios públicos: la salud y la educación. La transparencia y la privacidad son particularmente importantes en estos ámbitos, puesto que afectan a los grupos sociales más vulnerables, a quienes los gobiernos tienen el deber de proteger. La iniciativa podría extenderse con el tiempo a otras áreas de la administración pública en función de los resultados obtenidos en las pruebas piloto realizadas en los sectores de salud y educación.

POR QUÉ

El gasto público tiene un importante peso económico; representa el 12% del PIB en los países de la OCDE y hasta el 30% en los países en desarrollo.[88] Destinar parte del gasto público a empresas tecnológicas más responsables podría aumentar la visibilidad de las empresas *privacy-first* e impulsar nuevos mercados -liderados por el sector público- de empresas que no basan su negocio en la comercialización de los datos.

Además, aprovechar la contratación pública para promover modelos de negocio innovadores es una práctica recurrente. Durante años, la Comisión Europea ha solicitado la contratación pública de "bienes, servicios y obras con un impacto ambiental reducido a lo largo de su ciclo de vida".[89] Aparte de influir directamente en el medio ambiente, la contratación sostenible (GPP) ha beneficiado de muchas maneras a las regiones donde se ha puesto en marcha; por ejemplo, ha mejorado el desempeño ambiental y ha traído ventajas económicas, entre ellas la innovación industrial, el aumento de la competencia y la disminución de los precios.[90]

[88] Programa Ambiental de las Naciones Unidas, s. d.

[89] Ec.europa.eu 2019

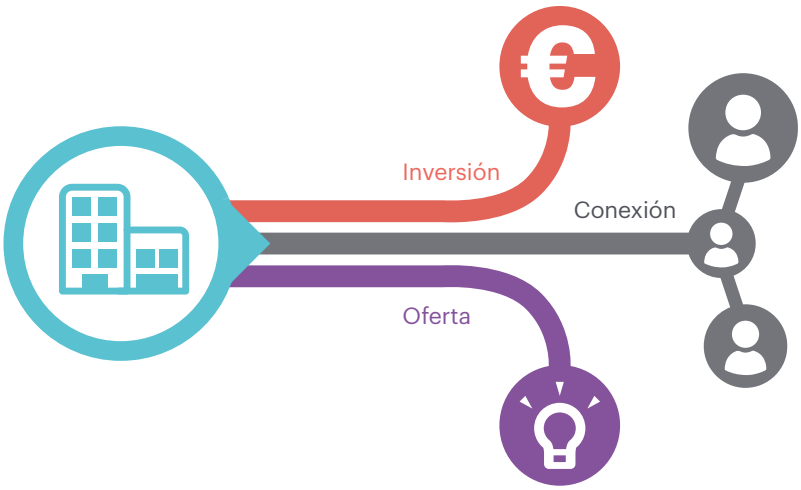
[90] Ibid.

CÓMO

Los responsables políticos pueden establecer un planteamiento regulador con requisitos flexibles que estimulen a las administraciones a contratar empresas privacy-first. Así, contratar a una empresa que respete la privacidad no sería un requisito obligatorio sino la opción predeterminada: los funcionarios responsables de las contrataciones deberían justificar por qué no lo hacen.

Para promover aún más la contratación de empresas *privacy-first*, los auditores independientes o los investigadores de otros organismos podrían auditar y supervisar qué organismos o departamentos de la administración pública contratan a este tipo de empresas.

Iniciativa 3: una red global de incubadoras de empresas *privacy-first*



QUÉ

Las incubadoras de empresas pueden ser fundamentales para estimular un sector o un tipo de empresa emergente, como la tecnología financiera (FinTech). Si bien muchas de ellas están financiadas por el sector privado, existen incubadoras y redes de emprendimiento financiadas con recursos públicos. Un ejemplo es EIT Climate-KIC, un programa apoyado por la Comisión Europea cuyo objetivo es acelerar la transición hacia una economía neutra en carbono.[91] A través de iniciativas específicas dirigidas a emprendedores con ideas de negocio centradas en el clima, este programa apoya el desarrollo de negocios y organiza concursos internacionales que premian las mejores ideas. Desde su lanzamiento en 2009, Climate-KIC ha apoyado a 2.000 empresas de nueva creación, dando lugar a una de las comunidades empresariales más grandes del mundo.[92]

[91] Climate-kic.org 2019

[92] Ibid.

Siguiendo el modelo de Climate-KIC, podría crearse una red global de incubadoras de empresas *privacy-first* con el fin de:

- Apoyar y financiar ideas de negocio exclusivamente enfocadas en la privacidad. Las iniciativas deben ser proyectos abiertos, que puedan reproducirse en otros ámbitos y crecer en magnitud y que además ofrezcan soluciones de privacidad, seguridad y transparencia a sus usuarios.
- Construir un ecosistema internacional de empresas digitales centradas en la privacidad, la confianza y la transparencia en el uso de los datos.
- Crear un espacio físico de colaboración (para terceros) que coincida con los valores de privacidad.

POR QUÉ

Una de las mayores dificultades a las que se enfrentan las empresas que respetan la privacidad es la financiación. La creación de una incubadora que apoye específicamente este tipo de negocios puede promover el contacto con inversores a los que les preocupa el impacto social, un perfil también al alza.[93]

Una incubadora dedicada a las empresas digitales centradas en la privacidad también serviría para controlar la evolución de estas empresas y garantizar que se mantengan fieles a sus valores iniciales.[94]

Además de apoyar a los emprendedores participantes, una incubadora *privacy-first* podría normalizar el uso responsable de los datos entre los jóvenes emprendedores del sector de la tecnología. Una incubadora centrada en este tipo de empresas podría contribuir a que el sector tecnológico evolucionase hacia un nuevo marco de valores que tuviera en la privacidad, la transparencia y la confianza sus objetivos primordiales.

Por otra parte, la incubadora podría ser el núcleo de una red mundial de proyectos similares que alimentaran el ecosistema y ayudaran a crear un nuevo paradigma internacional de negocio digital.

Ese ecosistema no sólo podría actuar de espacio neutral donde colaboraran las diversas partes implicadas (sectores público y privado, instituciones de investigación y entidades sociales), sino que además facilitaría la creación de equipos diversos. Por ejemplo, una red de incubadoras puede servir de canal a través del cual vincular la tecnología que prime la privacidad con las necesidades de los gobiernos en ámbitos como la salud, la educación, el medio ambiente, etc. Estas colaboraciones pueden concebirse de manera que generen soluciones útiles que primen la privacidad y que puedan aplicarse a gran escala y adaptarse a diferentes realidades y contextos culturales.

[93] Preston y James 2019

[94] Nesta 2014

CÓMO

La hoja de ruta para la creación de una red mundial de incubadoras de empresas *privacy-first* implica un planteamiento paso a paso.

1. El primer paso consiste en identificar a los principales interesados del ámbito académico y las organizaciones regionales del sector público y privado (concretamente empresas *privacy-first* como las analizadas en la sección 2 para que se unan a la iniciativa).

2. Formar una comisión asesora que redacte y valide una declaración centrada en la privacidad o documento de referencia en el que se establezcan los requisitos que deberán cumplir las empresas interesadas para poder participar.

3. El respaldo y el apoyo financiero de los gobiernos más los recursos institucionales ya existentes deben canalizarse hacia la red de incubadoras. Para impulsar la red global los gobiernos pueden elegir a gobiernos municipales que ya tengan un fuerte ecosistema empresarial. La red global puede trabajar con las ya existentes, por ejemplo los centros de desarrollo de pequeñas empresas de Estados Unidos o la Red de Centros Europeos de Empresas e Innovación. En lugar de empezar de cero, estas redes lideradas por el sector público pueden convertirse en un punto de referencia para la elaboración de planes de negocios y brindar apoyo administrativo, contable y jurídico a las empresas *privacy-first*.

4. Poner en marcha la declaración, la red y la financiación dirigida a las principales incubadoras a través de una convocatoria abierta de soluciones empresariales que primen la privacidad.

5. Se extendería a todo el mundo a través de eventos (encuentros de programadores, ferias profesionales, conferencias o premios) que atrajeran a nuevos socios a la red.

Incubar las empresas *privacy-first* con recursos públicos garantizaría que los fondos públicos se destinasen a iniciativas con repercusión social, en este caso, la protección de los datos de los ciudadanos. En este sentido podría plantearse el reto de tener que garantizar que los modelos comerciales respetuosos con la privacidad no deriven en modelos de extracción de datos una vez completada la fase de incubación.

Conclusión

Hacia un futuro digital *privacy-first*

A través de un análisis exhaustivo, el presente informe presenta un nuevo tipo de empresa en alza, capaz de ofrecer productos y servicios digitales de manera rentable sin recurrir a prácticas invasivas de tratamiento de datos: las empresas que anteponen la privacidad o *privacy-first*. Los retos a los que se enfrentan estas son los mismos que los de cualquier pequeña empresa que entra en un mercado monopolístico. Con todo, un mayor reconocimiento, sumado a los recursos financieros necesarios que permitan defender su propuesta basada en valores, podrían impulsar el éxito de esas empresas y, al mismo tiempo, ofrecer un argumento competitivo a favor de un Internet más privado.

La competencia es feroz. Los negocios *privacy-first* sólo tienen a su favor el creciente cuestionamiento público de las prácticas de las grandes empresas tecnológicas, que al parecer disponen de recursos ilimitados para influir en las normativas y marcar en rumbo del sector de la tecnología. A pesar de todo, este informe demuestra que las empresas privacy-first pueden entrar en el terreno de juego. Al igual que otras iniciativas basadas en valores, tratan de demostrar que la privacidad y el beneficio no son mutuamente excluyentes, una tarea nada fácil teniendo en cuenta que la cultura actual favorece a las empresas con potencial de crecimiento exponencial.

Las empresas *privacy-first* tienen potencial, por eso las iniciativas ideadas por el grupo de trabajo tratan de abordar a qué necesidades específicas se enfrentan, por ejemplo mayor visibilidad y disponibilidad de recursos. Las tres iniciativas propuestas (certificación, directrices de contratación pública e incubadoras) se basan, todas ellas, en herramientas ya existentes y probadas previamente para incentivar otros sectores, como la economía ecológica. Aunque no sean nuevas, las iniciativas se han adaptado para que los responsables de formulación de políticas puedan aplicarlas a cada contexto concreto.

Dada la rapidez a la que avanzan los cambios tecnológicos, los próximos años son cruciales para la supervivencia del incipiente ecosistema fundamentado en la privacidad. Para alimentarlo eficazmente, los responsables políticos tienen que poder identificar y comprender las complejidades de estos los modelos de negocio y aprovechar los incentivos. Y lo más importante de todo: deben reconocer el valor inherente y la experiencia con la que ya cuentan las empresas que anteponen la privacidad y son rentables, por ejemplo las descritas en este informe, ya que sólo así podrán ayudar a otras empresas *privacy-first* a prosperar.

Referencias

Agencia Europea de Seguridad de las Redes y de la Información . (2018). Recommendations on shaping technology according to GDPR provisions. [online]. Disponible en: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

Asher Hamilton, I. (2018). Tim Cook mounted his most stinging attack yet on tech firms that hoard 'industrial' quantities of data. Business Insider. [online] Disponible en: https://www.businessinsider.es/apple-ceo-tim-cook-attacks-tech-firms-that-hoard-data-2018-10?r=US&IR=T

Bcorporation.net. (2019). Certified B Corporation. [online] Disponible en: https://bcorporation.net/

Bhartiya, S., (2016.) Dark cloud looms over ownCloud as founder resigns. CIO. [online] Disponible en: https://www.cio.com/article/3063519/dark-cloud-looms-over-owncloud-as-founder-resigns.html

Brandel, J., Zepeda, M., Scholz, A. y Williams, A. (2017). Zebras: Let's Get In Formation. Medium. [online] Disponible en: https://medium.com/@sexandstartups/zebras-lets-get-in-formation-fdcbc72fec4a

Burnham, B., (2011). Duck Duck Go. Union Square Ventures. [online] Disponible en: https://www.usv.com/writing/2011/10/duck-duck-go

Chan, N., (2019). 259: Taking on Google, with Gabriel Weinberg, Founder of Privacy Browser DuckDuckGo. Foundr. [online] Disponible en: https://foundr.com/gabriel-weinberg-duckduckgo

Climate-kic.org, (2019). Entrepreneurship - Climate-KIC. [online] Disponible en: https://www.climate-kic.org/programmes/entrepreneurship

Climate-kic.org, (2019). KIC: The EU's main climate innovation initiative. Climate-KIC. The EU's main climate innovation innovation initiative. [online] Disponible en: https://www.climate-kic.org

Couldry, N. (2016). The price of connection: 'surveillance capitalism'. The Conversation. [online] Disponible en: https://theconversation.com/the-price-of-connection-surveillance-capitalism-64124

Digitalcooperation.org. (2019). The age of digital interdependence. [PDF] Disponible en: https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf

DuckDuckGo. (2019). Open Source Overview. [online] Disponible en: https://help.duckduckgo.com/duckduckgo-help-pages/open-source/opensource-overview

DuckDuckGo, (2019). DuckDuckGo Privacy. DuckDuckGo. [online] Disponible en: https://duckduckgo.com/privacy

DuckDuckGo, (2019). Privacy, simplified. - DuckDuckGo Browser Extension & Mobile App. DuckDuckGo. [online] Disponible en: https://duckduckgo.com/app

Downes, L. (2019). GDPR and the End of the Internet's Grand Bargain. Harvard Business Review. [online] Disponible en: https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain

Ec.europa.eu, (2019). Benefits of GPP. Benefits - GPP - Environment – Comisión Europea. [online] Disponible en: https://ec.europa.eu/environment/gpp/benefits_en.htm

Edelman, (2019). Earned Brand 2018. Edelman. [online] Disponible en: https://www.edelman.com/earned-brand

Etherington, D., (2019). Apple is now the privacy-as-a-service company. TechCrunch. [online] Disponible en: https://techcrunch.com/2019/06/03/apple-is-now-the-privacy-as-a-service-company

Faravelon, A., Frenot, S. y Grumbach, S. (2015). Chasing Data in the Intermediation Era: Economy and Security at Stake. IEEE Security & Privacy. [PDF] Disponible en: https://www.researchgate.net/publication/281599782_Chasing_Data_in_the_Intermediation_Era_Economy_and_Security_at_Stake

Fussell, S., 2019. Google's Totally Creepy, Totally Legal Health-Data Harvesting. The Atlantic. [online] Disponible en: https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999

GDPR.eu. (2019). What are the GDPR consent requirements? - GDPR.eu. [online] Disponible en: https://gdpr.eu/gdpr-consent-requirements/

Github, (2019). DuckDuckGo. GitHub. [online] Disponible en: https://github.com/duckduckgo

Goujard, C., (2018). France is ditching Google to reclaim its online independence. WIRED. [online] Disponible en: https://www.wired.co.uk/article/google-france-silicon-valley

StatcCounter. (2019). Search Engine Market Share Worldwide. StatCounter Global Stats. [online] Disponible en: https://gs.statcounter.com/search-engine-market-share#yearly-2019-2019-bar

GSMA. (2018). The Data Value Chain. [PDF] Disponible en: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf

Herrle, J. e Hirsh, J. (2019). The Peril and Potential of the GDPR. Centre for International Governance Innovation. [online] Disponible en: https://www.cigionline.org/articles/peril-and-potential-gdpr

Infobae. (2016). El Gobierno utilizará la versión corporativa de Facebook para agilizar el trabajo interno. [online] Disponible en: https://www.infobae.com/2016/02/16/1790481-el-gobierno-utilizara-la-version-corporativa-facebook-agilizar-el-trabajo-interno

International Data Corporation (2019) IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $189.1 Billion This Year with Double-Digit Annual Growth Through 2022. International Data Corporation (IDC). [online] Disponible en: https://www.idc.com/getdoc.jsp?containerId=prUS44998419.

Johnson, A., 2017. Massive phishing attack targets millions of Gmail users. CNBC. [online] Disponible en: https://www.cnbc.com/2017/05/04/gmail-google-hack-phishing-attack.html

Jones, H., (2018). Dr. Ann Cavoukian: Why Big Business Should Proactively Build for Privacy. Forbes. [online] Disponible en: https://www.forbes.com/sites/cognitiveworld/2018/08/17/ann-cavoukian-why-big-business-should-proactively-build-for-privacy/#92dcc5c2e3d8>

Karlitschek, F., (2016). Big changes: I am leaving ownCloud, Inc. today. Frank Karlitschek RSS. [online] Disponible en: https://karlitschek.de/2016/04/big-changes-i-am-leaving-owncloud-inc-today

Lomas, N., (2018). DuckDuckGo gets $10M from Omers for global privacy push. TechCrunch. [online] Disponible en: https://techcrunch.com/2018/08/29/duckduckgo-gets-10m-from-omers-for-global-privacy-push

Lomas, N., (2018). Pro-privacy search engine DuckDuckGo hits 30M daily searches, up 50% in a year. TechCrunch. [online] Disponible en: https://techcrunch.com/2018/10/11/pro-privacy-search-engine-duckduckgo-hits-30m-daily-searches-up-50-in-a-year/

Lomas, N., 2019. EU contracts with Microsoft raising 'serious' data concerns, says watchdog. TechCrunch. [online] Disponible en: https://techcrunch.com/2019/10/21/eu-contracts-with-microsoft-raising-serious-data-concerns-says-watchdog

Ly, W., Nirei, M., y Yamana, K. (2019). Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy. The Research Institute of Economy, Trade and Industry. [PDF] Disponible en: https://www.rieti.go.jp/en/publications/summary/19030027.html

Matomo (2019). Matomo Security Bug Bounty Programme. Matomo. [online] Disponible en: https://matomo.org/security

Matomo, (2019). New to Piwik FAQ - Analytics Platform. Matomo. [online] Disponible en: https://matomo.org/faq/new-to-piwik/#faq_130

Mazzucato, M. (2015). From Market Fixing to Market-Creating: A New Framework for Economic Policy. SPRU Working Paper Series (SWPS), 2015-25: 1-19. [PDF] Disponible en: https://www.sussex.ac.uk/webteam/gateway/file.php?name=2015-25-swps-mazzucato.pdf&site=25

Mazzucato, M., (2017). The entrepreneurial state. [PDF] Disponible en: https://marianamazzucato.com/wp-content/uploads/2017/02/US-ES-intro.pdf

Montgomery, M., (2019). Techlash Backlash? Next Generation of Startups Infusing Ethics Into Its Roots. Forbes [online] Disponible en: https://www.forbes.com/sites/mikemontgomery/2019/11/19/techlash-backlash-next-generation-of-startups-infusing-ethics-into-its-roots/#11cb18a04c16

Mozilla, (2019). An open source alternative for "the cloud". [online] The Internet Health Report 2019. Disponible en: https://internethealthreport.org/2019/an-open-source-alternative-for-the-cloud

Naughton, J. (2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. The Guardian. [online] Disponible en: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Nesta, (2014). Startup Accelerator Programmes. A Practice Guide. [PDF] Disponible en: https://media.nesta.org.uk/documents/startup_accelerator_programmes_practice_guide.pdf

Newman, J., (2018). The Dream of a Privacy-First Social Network: 6 Alternatives to Facebook. Fast Company. [online] Disponible en: https://www.fastcompany.com/40559106/the-privacy-first-social-network-a-great-idea-that-never-works

Nextcloud, (2019). EU governments choose independence from US cloud providers with Nextcloud. [online] Disponible en: https://nextcloud.com/blog/eu-governments-choose-independence-from-us-cloud-providers-with-nextcloud/

Nextcloud, (2019). How Nextcloud keeps your data secure. Nextcloud. [online] Disponible en: https://nextcloud.com/secure

Nytimes.com. (2019). Opinión | The New Terminology for Privacy. [online] Disponible en: https://www.nytimes.com/interactive/2019/04/10/opinion/internet-privacy-terms.html

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA l. Rev., 57, 1701.

Opensource.org. (2019). The Open Source Definition | Open Source Initiative. [online] Disponible en: https://opensource.org/osd

OpenX, (2019). About OpenX: Global Leader in Programmatic Advertising. OpenX. [online] Disponible en: https://www.openx.com/company/

Piwik, (2019). Piwik is now Matomo! [online] Disponible en: https://piwik.com/

Poortvilet, J., (2019). Nextcloud Conference 2019 talks now online. [online] Nextcloud. Disponible en: https://nextcloud.com/blog/nextcloud-conference-2019-talks-now-online

Poortvliet Feed, J., (2016). Building a business on a solid open source model. Opensource.com. [online] Disponible en: https://opensource.com/business/16/6/building-business-solid-open-source-model

Preston, M. y James, M. (2019). What Does the Growth of Impact Investing Mean? Harvard Law School Forum on Corporate Governance and Financial Regulation. [online] Disponible en: https://corpgov.law.harvard.edu/2019/11/10/what-does-the-growth-of-impact-investing-mean/

PrivacySpy. (2019). About | PrivacySpy. [online] Disponible en: https://privacyspy.org/about/

Protonmail, (2015). Is ProtonMail trustworthy? Our thoughts on email trust. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/is-protonmail-trustworthy/

Protonmail, (2015). ProtonMail Open Source Cryptography. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/protonmail-open-source-crytography/

Protonmail, (2019). Pricing. ProtonMail. [online] Disponible en: https://protonmail.com/pricing

Protonmail, (2019). ProtonMail is expanding access to more Android users. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/android-expansion/

Raicu, I. (2016). Young adults take more security measures for their online privacy than their elders. Vox. [online] Disponible en: https://www.vox.com/2016/11/2/13390458/young-millennials-oversharing-security-digital-online-privacy

Reglamento General de Protección de Datos (RGPD). (2019). Art. 83 RGPD: Condiciones generales para la imposición de multas administrativas | Reglamento General de Protección de Datos (RGPD). [online] Disponible en: https://www.privacy-regulation.eu/es/83.htm

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. Big Data & Society, 6(1).

Sawers, P. (2018). How ProtonMail is pushing email privacy standards. VentureBeat. [online] Disponible en: https://venturebeat.com/2018/05/13/how-protonmail-is-pushing-email-privacy-standards

Schacklett, M. (2018). 5 ways to avoid vendor lock-in. TechRepublic. [online] Disponible en: https://www.techrepublic.com/article/5-ways-to-avoid-vendor-lock-in/

Schwab, K., (2019). It's time to ditch Google Analytics. Fast Company. [online] Disponible en: https://www.fastcompany.com/90300072/its-time-to-ditch-google-analytics

Sec.gov. (2006). [online] Disponible en: https://www.sec.gov/Archives/edgar/data/1142701/000110465906033409/a06-9620_110q.htm

Slade, H., (2014). The Only Email System The NSA Can't Access. Forbes. [online] Disponible en: https://www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/#728c6c0867f7

Sugiyama, S. (2019). Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20. The Japan Times. [online] Disponible en: https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/#.XfoXimRKiUl

Thatoneprivacysite.net, (2019). VPN Comparison. That One Privacy Site. [online] Disponible en: https://thatoneprivacysite.net

Programa de las Naciones Unidas para el Medio Ambiente. (s. d.). Política de consumo y producción sostenibles. [online] Disponible en: https://www.un.org/sustainabledevelopment/es/sustainable-consumption-production/

Un.org. (2019). Data Economy: Radical transformation or dystopia? [PDF] Disponible en: https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf

Unctad.org. 2019. Data Protection and Privacy Legislation Worldwide. UNCTAD. [online] Disponible en: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Until.un.org. (2019). Home Technology Innovation Labs. United Nations. [online] Disponible en: https://until.un.org

Volpi, M., (2019). How open-source software took over the world. [online] TechCrunch. Disponible en: https://techcrunch.com/2019/01/12/how-open-source-software-took-over-the-world

Wachter, S. (2019). Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. SSRN Electronic Journal.

Weinberg, G., (2011). Are you chasing a fad or a market? Gabriel Weinberg's blog. [online] Disponible en: https://web.archive.org/web/20181204131004/https://ye.gg/blog/2011/04/are-you-chasing-a-fad-or-a-market.html

Wilson, M. y Graham, M. (2013). Neogeography and Volunteered Geographic Information: A Conversation with Michael Goodchild and Andrew Turner. Environment and Planning A: Economy and Space, 45(1), pp.10-18.

Wolford, B., (2019). Using ProtonMail for Journalism. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/journalism

Yen, A., (2015). ProtonMail has raised $2M USD to protect online privacy. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/protonmail-has-raised-2m-usd-to-protect-online-privacy

Yen, A., (2018). A look back at 2018 and our vision for the future of ProtonMail. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/2018-recap-future-roadmap

Yen, A., (2019). We have been awarded €2 million from the EU to further develop the Proton ecosystem. Blog de ProtonMail. [online] Disponible en: https://protonmail.com/blog/eu-funding

Zebras Unite. (2019). Zebras Unite. [online] Disponible en: https://www.zebrasunite.com

Zuboff, S. (2019). The age of surveillance capitalism. London: Profile Books, pp.75-77.

Agradecimientos

Autor principal

- **Tanya Álvarez** - Investigadora, Digital Future Society Think Tank

Colaboradores expertos

Este informe ha sido posible gracias a las ideas y aportaciones de los siguientes expertos:

- **Ali Hussein** - Kenya ICT Action Network (KICTANET)
- **Ayden Ferderline** - Mozilla Fellow
- **Carles Barreiro Bertolí** - abogado y DPD, Colegio de Abogados de Barcelona (ICAB)
- **Cristian Barrué** - investigador posdoctoral, Universitat Politècnica de Catalunya
- **Molly Wilson** - investigadora y diseñadora ejecutiva, Simply Secure
- **Pieter van Boheemen** - investigador, Rathenau Instituut
- **Renata Ávila** - directora, Ciudadanía Inteligente
- **Tetsuro Narita** - Banco Interamericano de Desarrollo
- **Frank Karlitschek** - fundador, Nextcloud
- **Johnny Ryan** - director de política y relaciones con la industria, Brave
- **Mattieu Aubry** - fundador, Innocraft
- **R. Miles Mccain** - fundador, Privacy Spy
- **Rory Donnelly** - CEO, Digi.Me
- **Linnet Taylor** - profesora adjunta, Tilburg Law School

Equipo del Digital Future Society Think Tank

Se agradece el trabajo editorial y las aportaciones de las siguientes miembros del equipo:

- **Carina Lopes** - Directora, Digital Future Society Think Tank
- **Olivia Blanchard** - Investigadora, Digital Future Society Think Tank
- **Nicole Harper** - Editora, Digital Future Society Think Tank

Citación

Por favor, cite este informe de la siguiente manera:

- Digital Future Society. (2019). *Privacy-first*: un nuevo modelo de negocio para la era digital. Barcelona, España.

Anexos

Anexo I: cómo detectar empresas *privacy-first*

Los siguientes rasgos pueden ayudar a identificar cuándo una empresa antepone la privacidad:

1 Perspectiva centrada en el usuario: el usuario es el principal beneficiario de este modelo

- El usuario controla totalmente sus datos, excepto cuando la ley obliga a la empresa a revelar ciertos datos.
- El negocio está diseñado para no recopilar ningún dato o sólo una pequeña parte. La empresa puede demostrar que sólo recopila el mínimo de datos necesarios para prestar su servicio.
- Estas empresas ofrecen al usuario la posibilidad de almacenar los datos exclusivamente en su dispositivo o en la nube o un servidor a los que la empresa no tiene acceso directo. Hacen públicas las medidas de seguridad adoptadas si los datos se almacenan fuera del dispositivo/servidor del usuario y sólo conservan los datos durante el tiempo mínimo y estrictamente necesario.
- La empresa permite a los usuarios decidir si quieren que el *software* o el servicio utilicen sus datos.

2 Comunicación clara

- Al usuario se le informa de cada etapa del procesamiento de datos. El lenguaje utilizado para explicar qué tipo de datos se recopilan, cómo se recopilan y con qué fin, cómo se tratan y de qué manera puede el usuario controlarlos (si procede) es sencillo y directo.

3 Privacidad desde el diseño

- Las empresas aplican la privacidad desde el diseño. El producto o servicio protege la privacidad del usuario por defecto.

4 Procesamiento de datos acordado

- Dado que las empresas *privacy-first* gestionan la mínima cantidad de datos personales posible, el tratamiento de datos fuera de la empresa es muy poco frecuente o inexistente. Si participa un tercero, los datos que somete a tratamiento no se pueden rastrear al no ser identificables. La empresa controla a cualquier tercero que colabore con ella y solicite acceso a los datos de los usuarios.

5 Seguridad

- La seguridad de los datos forma parte de la propuesta de valor de la empresa. El protocolo de seguridad es transparente y está a la vista de todos.

6 Rendición de cuentas

- La empresa ha establecido medidas técnicas y organizativas que acreditan y certifican que la privacidad es su prioridad absoluta. Además, adopta un enfoque proactivo al comunicarse con la comunidad y las partes interesadas sobre cualquier cuestión relativa a la credibilidad de la empresa.

Anexo II: ¿qué son los datos personales?

Este informe analiza cómo puede un modelo de negocio generar ingresos sin utilizar datos personales. La siguiente tabla define las distintas categorías de datos que establece el actual RGPD.

<table>
<tr><td colspan="2">Datos personales: cualquier información pública o privada que se pueda rastrear o utilizar para identificar a una persona, directa o indirectamente. Ejemplos: rasgos culturales, físicos, sociales...</td><td rowspan="3">Datos no personales
La mayoría de datos generados, normalmente por máquinas o sistemas.

Ejemplos: datos de rendimiento, transacciones, datos individuales anonimizados.</td></tr>
<tr><td>Voluntarios: datos que una persona ha facilitado conscientemente.

Ejemplos: información confidencial facilitada a un banco o servicio de salud, por ejemplo el número de identificación o de seguridad social. Contenido de las redes sociales. También engloba los datos de ubicación si las aplicaciones cuentan con geolocalización de mensajes.[95]</td><td>Inferidos: nuevos datos derivados de información aportada voluntariamente y observada.

Datos que alimentan algoritmos que luego recomiendan productos a los usuarios, determinan la solvencia, crean perfiles, etc.</td></tr>
<tr><td>Observados: metadatos o datos de uso recogidos a través de los servicios que utiliza una persona.

Ejemplos: factura del teléfono móvil, parámetros de uso de un sitio web, ubicación, etc.</td></tr>
</table>

[95] Wilson y Graham 2013

Anexo III: Mapa del ecosistema mundial de empresas *privacy-first*

Privacidad, lo primero para los beneficios			
Nombre	**País**	**Tipo**	**Descripción**
Brave	EE.UU.	B2C/B2B	Brave: navegador de código abierto que bloquea los anuncios/"contenido no deseado" y protege la privacidad. Declara ser 8 veces más rápido que Chrome y Safari.
Cozycloud	Francia	B2C	Servidor privado que almacena datos y aplicaciones web personales. Además de ofrecer privacidad y seguridad, la empresa asegura que es un servicio de almacenamiento de datos inteligente y fácil de usar.
Clue	Alemania	B2C	Aplicación de seguimiento de la menstruación y la ovulación. Clue anonimiza los datos y los envía a instituciones de investigación para avanzar en el estudio de la salud y la fertilidad de la mujer.
Fathom	Sede en EE.UU.	B2C/B2B	Plataforma analítica respetuosa con la privacidad. Proporciona estadísticas útiles sobre los sitios web sin rastrear ni almacenar los datos personales de los usuarios. Anonimiza a los visitantes mediante almohadillas (#), no usa cookies y cumple los reglamentos RGPD/PECR.
MaidSafe	Escocia	B2C/B2B	El proyecto SAFE (Secure Access for Everyone, acceso seguro para todos) pretende sustituir el concepto de Internet centralizada y controlada por una red totalmente descentralizada y fiable. Se trata de un *software* de código abierto que crea una plataforma de Internet descentralizada. Internet P2P que ofrece a los usuarios una solución totalmente descentralizada.
OpenCollective	EE.UU.	B2C	Plataforma que permite a grupos y comunidades recoger dinero y pagar de manera transparente. Promueve la transparencia financiera. Ayuda a las organizaciones a recaudar dinero sin necesidad crear una cuenta bancaria o constituir una entidad legal.

Nombre	País	Tipo	Descripción
Purism	EE.UU.	B2C/B2B	Dispositivos informáticos enfocados a la seguridad. Ofrece paquetes de servicios/correo/redes sociales/VPN y servicios de encriptación de extremo a extremo. Desarrolla portátiles y teléfonos que protegen la privacidad. Todo el *software* es de código abierto y fácilmente verificable y todo el código fuente es público, sin puertas traseras ni necesidad de registrarse. Se puede modificar para adaptarlo a cualquier necesidad.
Threema	Suiza	B2B/B2C	Aplicación de mensajería instantánea encriptada de extremo a extremo que no solicita información personal identificable. Sus principales argumentos de venta tienen que ver con la privacidad (anonimato total, cifrado completo, política de privacidad transparente, etc.)
Tresorit	Hungría/ Suiza	B2B/B2C	Servicio de almacenamiento en la nube que refuerza la seguridad y la encriptación de los datos. Ayuda a las empresas a almacenar y compartir sus archivos y datos y a cumplir las exigencias de confidencialidad y privacidad.
Wickr	EE.UU.	B2B/B2G	Empresa de *software* conocida por su aplicación de mensajería instantánea de alta seguridad. También ofrecen una plataforma de comunicación completa, cifrada de extremo a extremo (marca Wickr Pro).
Qwant	Francia	B2C	Motor de búsqueda que cuenta con un motor de indexación propio (ubicado únicamente en la UE); asegura no rastrear a los usuarios y evitar el filtro burbuja (las búsquedas no son personalizadas). Motor de búsqueda fácil de usar, de uso libre y que respeta la privacidad. "Qwant junior" para niños (resultados filtrados).

Privacidad, lo primero para las organizaciones sin ánimo de lucro		
Nombre	**País**	**Descripción**
Freenet	N/A	Plataforma P2P que evita la censura a través de un almacén de datos distribuido y descentralizado que guarda y muestra la información. La comunicación se codifica y se reenvía a través de otros nodos para que sea extremadamente difícil determinar quién solicita la información y cuál es su contenido.
Midata	Suiza	Cooperativa que permite a las personas controlar sus datos médicos. Los usuarios pueden almacenarlos con seguridad, seguir su evolución y, si lo desean, facilitarlos al médico, la familia o estudios clínicos. Plataforma que deja en manos de los usuarios destinar sus datos a la investigación de la salud.
OpenStreetMap	Reino Unido	Proyecto colaborativo cuyo objetivo es crear un mapa libre y editable de todo el mundo. Los mapas se basan en datos participativos recabados por los usuarios y pueden utilizarse posteriormente para crear documentos y mapas digitales. Mapa colaborativo libre y abierto con información detallada.
Securedrop	N/A	Plataforma de comunicación segura entre medios de comunicación/ periodistas y denunciantes (fuentes expuestas). Práctica herramienta que permite a los medios de comunicación recibir documentos de fuentes anónimas.
Signal	EE.UU.	Servicio de mensajería encriptada que puede utilizarse para la comunicación entre personas y grupos. Los usuarios pueden verificar la identidad de los contactos y la integridad del canal de datos. Aplicación de mensajería simple, gratuita y segura que funciona en cualquier plataforma móvil.
Solid	EE.UU.	Plataforma dirigida por Tim Berners Lee que permite a los usuarios leer y crear contenido y a la vez gestionar el acceso a los datos. Los usuarios controlan los datos y deciden qué aplicaciones tienen acceso a ellos.
Telegram	Reino Unido/EAU	Servicio de mensajería y voz por IP basado en la nube compatible con los principales sistemas operativos. La aplicación permite enviar mensajes, fotos, vídeos, audio y cualquier otro tipo de archivo. Los usuarios pueden acceder a los mensajes y archivos desde varios dispositivos y compartir fotos de gran tamaño.


Digital
Future Society