ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

19/2022 marzo de 2022

David Ramírez Morán

Fronteras de la materia prima digital

Fronteras de la materia prima digital

Resumen:

Una de las principales materias primas de la revolución 4.0 son los datos. Su obtención es una actividad compleja que se está realizando por diversos procedimientos desde la captura directa a la instrumentalización de otros servicios para conseguir datos adicionales. Tampoco puede olvidarse que existen técnicas que permiten obtener datos de forma ilegítima y que esta falta de legitimidad puede ser el resultado de distintas cuestiones como son la violación de la privacidad personal, el incumplimiento de la legislación sobre protección y tratamiento de datos, la violación de las medidas de protección de la información o de operaciones de espionaje dirigidas incluso por Estados.

Los datos de los ciudadanos son requeridos por los nuevos modelos de negocio que la revolución industrial 4.0 está generando. Disponer de los datos puede resultar imprescindible para conseguir la productividad con la que asegurar la prosperidad de los Estados. Por este motivo, la gestión de los datos alcanza una naturaleza estratégica que puede afectar a los intereses nacionales, más allá de cuestiones tan importantes como los derechos de los ciudadanos a la privacidad. Las fronteras al uso de los datos surgen de forma natural debido a las distintas regulaciones existentes así como a las diferencias existentes entre los principios que rigen las sociedades.

Palabras clave:

Privacidad, protección de datos, intereses económicos, ética.

Borders for the digital raw materials

Abstract:

Data is one of the main raw materials for the 4.0 industrial revolution. Its extraction is a complex activity that is being done through different procedures, from direct capture to the instrumentation of other services to obtain additional data. It should not be forgotten that techniques exist to obtain data illegally and that this lack of legitimacy arises from different questions such as the violation of personal privacy, the lack of compliance of the protection and processing of date, the violation of the information protection measures or spying operations driven even by States.

Citizens' data, both of those belonging to a State or of foreign citizens, are required by the new business models that the 4.0 industrial revolution is generating. Having the data may result a requirement to achieve the productivity that ensures the prosperity of a State. For this reason, the management of data reaches a strategic nature that may affect national interests, beyond matters as important as the rights of citizens for privacy.

The borders to the use of data arise in a natural way as a result of the different existing regulations as well as the existing differences between the principles that drive the societies.

Keywords:

Privacy, data protection, economic interest, ethics.

Cómo citar este documento:

RAMÍREZ MORÁN, David. *Fronteras de la materia prima digital*. Documento de Análisis IEEE 19/2022.
https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA19_2022_DAVRAM_Fronteras.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

La materia prima necesaria para el desarrollo de productos digitales son los datos. Sin ellos no existe posibilidad alguna de alcanzar los beneficios que la transformación digital puede aportar a la sociedad. Los datos se están generando continuamente y se están refinando para que resulten de utilidad en la optimización de los procesos productivos y en el desarrollo de nuevos modelos de relación y negocio.

El paso inicial para que un dato pueda utilizarse en etapas posteriores de la cadena es su captación y digitalización. A partir de ese momento, si el proceso se ha realizado correctamente en términos de precisión y calidad, se habrá convertido de un elemento de información que, si bien puede ser simple o poco significativo de por sí, resulta imprescindible para que los complejos sistemas de tratamiento y utilización de la información puedan realizar su función y resultar de utilidad.

Obtener datos requiere, por un lado, un sensor, un elemento que genere ese dato en un formato que posteriormente pueda ser procesado; y, por otro lado, un sistema encargado de la recopilación de esos datos para ponerlos a disposición de los encargados de su procesado. En el caso de datos industriales o científicos, son los profesionales los encargados de dotarse de estos dos elementos para llevar a cabo su labor. Sin embargo, con los datos fruto de la actividad de las personas, donde actualmente recae el mayor interés por parte de organizaciones públicas y privadas, la solución no es tan sencilla. Por defecto, los datos no surgen por arte de birlibirloque, perfectamente ordenados y validados en bases de datos accesibles fácilmente para su tratamiento.

La combinación de Internet, los servicios digitales y los teléfonos móviles han dado respuesta a este problema proporcionando un sensor, que es el teléfono, una forma de recopilar los datos mediante Internet y unos sistemas que los reciben y almacenan cuando se hace uso de los servicios digitales disponibles a través de Internet. Esta aproximación proporciona una infraestructura, los medios materiales que hacen posible la recopilación de datos para su tratamiento posterior, aunque falta aún otra parte importante.

Para que la infraestructura sea útil, es necesario que las fuentes de datos, las menas, las personas, las utilicen; y es aquí donde la generalización del uso de los móviles e Internet y la aparición de más y más servicios digitales que facilitan el día a día de las personas toman importancia. Cada vez que se usa uno de estos servicios se están

generando datos, algunos más relevantes y otros menos en función de en qué esté interesado el prestador del servicio que los recopila.

Para prestar un servicio hay un conjunto de datos que resultan imprescindibles para el correcto funcionamiento técnico del servicio, como son el producto deseado, la información requerida para producirlo —como pudiera ser el modelo de producto solicitado, la localización actual o el origen y destino de un desplazamiento— los elementos de autorización necesarios para poder controlar el acceso a los servicios, los datos técnicos imprescindibles para llevar a cabo la comunicación, como la dirección IP del dispositivo y, opcionalmente, cierta información del dispositivo utilizado con objeto de proporcionar la mejor experiencia de usuario posible.

De todos estos datos imprescindibles, el prestador del servicio solo requeriría almacenar durante cierto tiempo algún modo de identificar el usuario y el servicio adquirido con fines de facturación. Por motivos de seguridad, la legislación impone requerimientos adicionales a la información que debe almacenarse de cada una de estas transacciones, requiriendo que los metadatos de la comunicación sean almacenados con fines de investigación ante posibles delitos. Son los operadores de comunicaciones los que detentan esta responsabilidad.

Hasta aquí se describe un modelo de negocio viable que, salvo por la digitalización, se lleva realizando desde que apareció el comercio de bienes y servicios en el mundo: un cliente requería el servicio, pagaba por él y finalizaba la relación entre ambas partes.

Desde finales del siglo XVIII hasta la actualidad, se produce una revolución de este modelo. La competencia hace que el cliente pueda elegir a qué proveedor recurrir y es necesario es necesario desarrollar estrategias que inciten al cliente a decantarse por uno u otro. En paralelo, la mejora de la calidad de vida hace que se soliciten productos mucho más allá de la mera subsistencia, cuyo mercado puede ampliarse mediante campañas que generen deseo. Ambos factores hacen que la publicidad aparezca como una nueva herramienta capaz de generar valor y dar lugar a un nuevo modelo de negocio. Durante el siglo XX, la publicidad ha sido una importante fuente de financiación de los medios de comunicación basada en una relación unidireccional. No se disponía de retroalimentación de los efectos más allá de observar la variación en el volumen de negocio generado. Además, la capacidad de personalizarla para hacer llegar el mensaje a las personas objetivo era muy limitada.

Con la llegada de las comunicaciones personales en primer lugar y con la explosión de Internet posterior es posible dirigirse específicamente a una persona y se produce una transformación total. La comunicación se puede hacer de forma individual, lo que requiere un mayor uso de recursos para contactar persona a persona frente a la publicación de un mero anuncio en un periódico, una cadena de radio o de televisión. Por eso es también necesario disponer de algún tipo de filtro que permita optimizar los recursos disponibles para dedicarlos a aquellos perfiles más proclives a convertirse en clientes. Surge la necesidad de contar con los datos de las personas y aparecen nuevos negocios que proporcionan lo que un proveedor de servicios necesita: colectivos segmentados por edad, características, intereses, etc. a los que dirigir las campañas.

Para segmentar a la población son necesarios sus datos y para ciertos negocios resulta relativamente sencillo contar con ellos tan pronto como haya existido una relación comercial previa. Sin embargo, para otros negocios o para hacer nuevos clientes, no existe solución hasta la aparición de estos negocios. Pero ¿cómo acceden a esta información? La llegada de la web 2.0 fue otra revolución. Los usuarios empezaban a generar contenidos y se generalizaba tanto el requerimiento de identificarse los usuarios como la generalización de técnicas para identificar a cada usuario individual.

En la actualidad, se está produciendo una evolución en Internet en la que los flujos de datos se dan la vuelta y es el proveedor el que recibe más información que el usuario. Con estos datos es con los que se están alimentando las nuevas tecnologías de aprendizaje máquina y de inteligencia artificial que regirán el futuro de la humanidad como preconizan los principales expertos de muchos sectores.

Perfilar y asociar información

Una de las medidas que permite incrementar la calidad de los datos para su tratamiento posterior es la clasificación. Toda información puede ser objeto de infinidad de clasificaciones diferentes y una de ellas es conseguir atribuir la información a una persona particular. A partir de información correctamente asociada a una persona es posible generar un perfil que defina los intereses, prácticas y costumbres de esa persona. Sin embargo, los riesgos que esta práctica conlleva saltan a la luz rápidamente cuando se consideran las posibles informaciones que se podrían extraer de los datos recopilados del uso de Internet de ese usuario. Cuestiones como salud, ideología política, datos

laborales… podrían extraerse de datos como las páginas web visitadas. A estos efectos se han desarrollado diversas técnicas que permiten tanto identificar el perfil al que asociar una información como trazar interacciones en distintas páginas web por parte de un mismo usuario.

Las cookies han sido, durante años, una de las principales herramientas para el rastreo de las acciones de los usuarios individuales a través de Internet. Consisten en dejar almacenado en el ordenador del usuario un pequeño paquete de información que posteriormente será leída al acceder a otras páginas web.

Para individualizar la información recabada de un dispositivo existen numerosas técnicas que permiten identificar unívocamente el dispositivo desde el que accede un usuario a una página web incluso aunque no haya proporcionado información como un nombre de usuario. Se denominan técnicas de *fingerprinting*[1] y consisten en implantar en las páginas web fragmentos de código con los que se recaba información sobre el tipo de tarjeta gráfica, las fuentes instaladas, las extensiones del navegador, el idioma configurado… Uno de los actores que más está dando visibilidad a las posibilidades de identificación y seguimiento de los usuarios es la Electronic Frontier Foundation[2] que permite realizar pruebas sobre la correcta configuración de los dispositivos para evitar estas técnicas de recopilación de información y perfilado de los usuarios.

Los servicios en línea requieren identificación previa incluso en las versiones gratuitas. El prestador quiere saber quién utiliza el servicio y cuándo lo utiliza. Esto permite el perfilado de los usuarios, lo que hace, de acuerdo con la normativa, que la información intercambiada en la prestación de ese servicio también tenga naturaleza de información personal. Las versiones gratuitas, especialmente en las aplicaciones para teléfonos móviles, constituyen también una herramienta para hacer llegar publicidad al usuario.

Cada vez son más las empresas y organizaciones que desarrollan aplicaciones propias para que sus usuarios y clientes se relacionen con ellas frente a la solución previa que consistía principalmente en la presencia en Internet. Estas aplicaciones cada vez proporcionan más funcionalidades y, paralelamente, requieren más permisos de acceso a la información de los terminales en los que se ejecutan. Información como la ubicación,

[1] Disponible en: https://fingerprintjs.com/blog/browser-fingerprinting-techniques/
[2] Disponible en: https://www.eff.org/

obtenida tanto de los sensores específicos como por medios indirectos de redes Wi-Fi visibles puede geolocalizar con precisión la ubicación del usuario.

En la actualidad, sobre todo en los países más desarrollados, el número de teléfono es prácticamente equivalente a una identificación personal de un ciudadano salvo los dispositivos utilizados con fines profesionales exclusivamente. El uso o remisión de este dato, en caso de tratarse de un dispositivo personal y no profesional, ya da lugar a que todos los datos intercambiados por la aplicación se consideren datos personales.

Ante los riesgos de suplantación, se están implantando mayores medidas de seguridad, como el segundo factor de autenticación que, en paralelo a permitir proporcionar los servicios con mayor seguridad, también supone una vía de fuga de información. Para el funcionamiento de estas herramientas se requiere información personal como, por ejemplo, el número de teléfono del usuario o su correo electrónico para recibir un código con el que reconfirmar que es el usuario el que está intentando acceder legítimamente a la aplicación. En otros casos lo que se solicita es la instalación de una aplicación específica en el dispositivo que generará claves con las que poder acceder. Esta aplicación puede requerir acceder a Internet, por lo que estaría remitiendo información sobre la dirección IP del usuario, además de que en muchos casos se desarrolla con permisos que pueden ir mucho más allá de la generación de una clave adicional para el acceso. Se pueden incluir funcionalidades como la geolocalización, que contribuye a la seguridad al atajar accesos del mismo usuario desde lugares muy distantes, pero que suponen una posible vía de obtención de datos para los prestadores del servicio sin más que registrar estas localizaciones.

Nuevamente es la seguridad el argumento esgrimido para su implantación, apelando al control de la edad de los usuarios para que no accedan a contenidos inadecuados por ejemplo en páginas de visualización de vídeos. A cambio, una plataforma de este tipo va a disponer de un historial de todos los vídeos que ese usuario ha visualizado.

Los correos electrónicos ya no son tan inocentes y todos los enlaces, generalmente remitidos por servicios que facilitan la distribución masiva, también constituyen un mecanismo de identificación de a quién ha llegado el mensaje, si ha pulsado los enlaces, etc. Para ello se envía un enlace distinto a cada usuario al que se ha remitido la información mientras que en el servidor se puede determinar qué usuario ha accedido a la información sin más que leer la información de la dirección URL requerida al pulsar el

usuario sobre el enlace. De similar manera, los correos electrónicos ya no son meros textos sin formato, sino páginas html completas. Esto permite incluir fuentes e imágenes cuya descarga del servidor se puede tanto registrar como individualizar para determinar quién y cuándo se ha leído un correo electrónico de no tomar medidas para evitarlo.

Una página web moderna tiene múltiples funcionalidades en las que, para su implementación, puede recurrirse a utilizar servicios en línea directamente integrados en la página que proporcionan otros proveedores. Elementos como cajas de búsqueda que utilizan buscadores tradicionales pero circunscritos a esa página web, herramientas de elaboración de estadísticas de visitas, utilización de fuentes individualizadas, servicios de distribución de contenidos que aceleran la navegación, etc. permiten facilitar la creación de la página recurriendo a soluciones ya desarrolladas. Como contrapartida, en la mayor parte de los casos es necesario recurrir a cargar código directamente de los servidores de estos proveedores. De esta forma, los proveedores van a obtener datos del usuario de la página web como la página web a la que están accediendo estadísticas sobre el tiempo que el usuario ha pasado en ella, incluso visualizaciones de la interacción del usuario con la página...

En general, toda interacción realizada actualmente en Internet está siendo registrada por uno o más proveedores que pueden hacer uso de la información. Por supuesto, el proveedor del servicio que estamos usando recibe la información. Sin embargo, quizá no resulte tan evidente que todos los otros proveedores de los que se descarga información para el funcionamiento de la página también van a recibir información sobre ese acceso.

No hay que olvidar que una *app* instalada en un dispositivo móvil es equivalente a una aplicación web que puede incorporar funcionalidades adicionales no permitidas en páginas web gracias a que está instalada en el dispositivo y a la que el usuario ha otorgado confianza al instalarla. Por lo tanto, el proveedor de la *app* tendrá acceso a mucha más información del usuario si así se lo ha permitido este, como pudiera ser acceso a los contenidos del dispositivo, un mayor control sobre funcionalidades como llamadas o envío y recepción de mensajes…

El paso más allá

Cuando una tercera persona desea acceder sin autorización del usuario a unos datos protegidos por los mecanismos de identificación es necesario aplicar técnicas de *cracking*[3]. Se trata de utilizar técnicas que evadan las medidas de protección para acceder a esa información protegida.

Estas herramientas se caracterizan por proporcionar un mecanismo que permite tomar el control total sobre los dispositivos en los que se consigue instalar. Para ello, aprovecha vulnerabilidades, fallos de funcionamiento del software de los dispositivos objetivo y consigue instalar programas que capturan la información del dispositivo y la remiten a las infraestructuras de almacenamiento y control que les dan soporte desplegadas en Internet. No solo se puede acceder a la información ya existente en el dispositivo como fotografías, correos electrónicos o listas de llamadas, sino que también es posible instalar, ejecutar, eliminar o modificar aplicaciones.

Mediante estas herramientas se pueden obtener contraseñas, acceder al micrófono o la cámara y remitir los audios y vídeos grabados, obtener los datos de múltiple factor de autenticación para acceder o hacer operaciones en servicios online… En pocas palabras, se pueden llevar a cabo todas las acciones que puede realizar el propietario del teléfono, e incluso más, sin su conocimiento.

Se trata de herramientas muy complejas que se enfrentan a unos dispositivos cada vez más seguros. La vulnerabilidad que permite la instalación de la herramienta, que para hacerlo se requiera la mínima intervención del usuario —a veces basta con acceder a una página web en un navegador—, la infraestructura que da soporte en Internet a la herramienta, el sigilo con el que envía los datos recabados y el soporte necesario para que la herramienta siga realizando su función, incluso tras ser detectados y arreglados los fallos que permitieron su instalación, constituyen el valor conseguido con el desarrollo de estas herramientas. Dos ejemplos de herramientas utilizadas con estos fines son Xkeyscore, mencionada en las filtraciones de Edward Snowden y que fue utilizada para

[3] Las acciones de cracking son aquellas que permiten llevar a cabo actividades no autorizadas en un sistema informático por parte de una tercera persona explotando vulnerabilidades detectadas o utilizando las credenciales obtenidas por medios ilícitos. Cabe resaltar la diferencia de este término con el *hacking*, que consiste en aprovechar las características de los sistemas informáticos para realizar o facilitar la realización de una labor mediante medios informáticos.

acceder al teléfono móvil de la canciller alemana Angela Merkel[4] y hasta 125 altos cargos más de su Gobierno, y la herramienta Pegasus, desarrollada por la empresa NSO de origen israelí.

Las potentes capacidades que proporciona la herramienta Pegasus, por ejemplo, suponen un riesgo para la privacidad de cualquier persona, lo que podría cuestionar el desarrollo de este tipo de tecnologías. Sin embargo, en el caso de la empresa NSO, se destaca en su página web[5] «NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe». De acuerdo con esta afirmación, solamente proporciona su tecnología a agencias gubernamentales por lo que asumen que el uso que de ellas se hará estará sujeto al respeto de la ley.

Sin embargo, Pegasus ha sido frecuentemente citada en los medios ante escándalos que se han producido por su uso contra individuos cuyo perfil no se corresponde con estos objetivos dado que han aparecido trazas de la herramienta en dispositivos de activistas, jefes de Gobierno, diplomáticos, periodistas…[6].

Estos hechos han llevado al supervisor de la Protección de Datos Europeo (European Data Protection Supervisor) a emitir un informe[7] en 2022 recomendando la prohibición del desarrollo y despliegue de este tipo de herramientas en el territorio de la Unión Europea para proteger los derechos fundamentales y libertades de los ciudadanos. Este mismo informe incluye la excepción de utilizarlas para prevenir amenazas inminentes muy serias, aunque destaca un conjunto de cuestiones que deben tenerse muy en cuenta incluso en estas situaciones excepcionales:

- Reforzar la supervisión democrática de las medidas de vigilancia.
- La implementación estricta del marco legal de protección de datos de la UE.

[4] "NSA tapped German Chancellery for decades, WikiLeaks claims". Disponible en: https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel Accedido 1/03/2022
[5] Disponible en: https://www.nsogroup.com/
[6] *Dana Priest*, *Craig Timberg* and *Souad Mekhennet*. "Private Israeli spyware used to hack cellphones of journalists, activists worldwide". Disponible en: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ Accedido el 5/3/2022
[7] "Preliminary remarks on Modern Spyware". European Data Protection Supervisor. Disponible en https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

- Supervisión judicial, tanto *ex-ante* como *ex-post*, que debería ser real, no una mera formalidad.
- Reforzamiento de las protecciones ofrecidas por el procedimiento criminal.
- Reducir el riesgo de que datos originados mediante estas prácticas de vigilancia abusiva y no democrática alcancen las bases de datos de la UE, como las de Europol o las de los cuerpos de seguridad de los Estados miembros.
- Parar el uso y abuso de los propósitos de seguridad nacional para legitimar vigilancia con motivaciones políticas.
- Abordar los problemas sobre el respeto de la ley.
- Empoderar a la sociedad civil para generar consciencia y que se genere debate público.

Tanto XKeyscore como Pegasus son herramientas teóricamente dirigidas a contribuir a la seguridad nacional, aunque no debe olvidarse que en el mundo cibernético hay numerosos actores mucho menos transparentes que también cuentan con las capacidades para desarrollar y desplegar este tipo de herramientas. Solo es cuestión de que exista suficiente interés sobre la información que un individuo maneja para que alguien, con el debido respaldo técnico y económico, decida utilizar una herramienta de este tipo para acceder a ella.

Riesgos para los intereses nacionales

Ante los riesgos que suponen la disponibilidad y tratamiento de los datos de carácter personal para los derechos considerados fundamentales en la UE como son la privacidad y la libertad de expresión, la normativa de protección de datos ha permitido establecer limitaciones sobre el uso que sobre los datos se podía hacer, así como los derechos que amparan a los usuarios en el caso de que su información haya sido registrada o tratada.

Orbitando sobre este día a día en el que el principal objetivo es obtener datos que alimenten los sistemas informáticos, también se está construyendo una arquitectura con la que es posible conocer más a través de la información que los usuarios proporcionan vehementemente. La privacidad de la información del individuo en ocasiones no le importa siquiera al individuo, que la utiliza de intercambio para la percepción gratuita, en

términos de coste económico, de servicios. Sin embargo, esta información, convenientemente agregada y procesada, puede proporcionar datos de gran valor para terceros con intereses que pueden no ser compatibles con los de la población que tan generosamente ha proporcionado sus datos, intereses, gustos, costumbres, opiniones, estado de salud, estado de ánimo e incluso capacidad económica.

Las normativas de protección de datos se centran en la protección de la información de carácter personal por lo que solo en aquellos casos en los que sea posible asociar un dato a un individuo se puede producir una vulneración.

La Regulación General de Protección de Datos[8] es la norma de la UE en vigor a este respecto y supone un escollo importante para actividades que tradicionalmente se habían venido llevando a cabo para la operación normal de servicios prestados desde países externos a la UE.

En octubre de 2015, se declaró inválido el International Safe Harbor Privacy Principles, un marco bajo el que se podía llevar a cabo la transferencia de información personal de Europa a Estados Unidos. Conocido como sentencia Schrems I, pronto se empezó con la elaboración de una segunda normativa que recibió el nombre de EU-US Privacy Shield. El Tribunal Europeo de Justicia también lo declaró inválido en octubre de 2020 con la sentencia denominada Schrems II. El TJCE dictaminó que el acuerdo transatlántico del Escudo de la Privacidad (Privacy Shield), que fijaba las normas para el intercambio de información entre la UE y Estados Unidos no era válido, porque no podía proteger los datos de los usuarios europeos ante legislaciones de Estados Unidos como el CLOUD Act[9], que requiere que las empresas estadounidenses proporcionen, por razones de seguridad nacional, información ubicada en sus servidores incluso aunque se encuentren ubicados más allá de sus fronteras. Sin embargo, el tribunal permitió a algunas empresas tecnológicas como AWS y Google utilizar los Cláusulas Contractuales Estándar (CCE) como mecanismo legal para las transferencias de datos, con algunos ajustes.

[8] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[9] Disponible en: www.justice.gov/CLOUDAct

Se encuentra en curso un nuevo marco para el intercambio de información personal entre UE y EE. UU. que en algunos foros se denomina Schrems III en alusión a los dos mecanismos previos en esta línea.

Las normativas sobre protección de datos también pueden constituir un riesgo económico para empresas que hacen del uso y tratamiento de los datos su modelo de negocio. Recientemente se informaba sobre los riesgos que una de las empresas de mayor capitalización bursátil mundial, Meta, había detectado con la regulación de protección de datos europea: «reliance on Standard Contractual Clauses in respect of European user data does not achieve compliance with the General Data Protection Regulation (GDPR) and preliminarily proposed that such transfers of user data from the European Union to the United States should therefore be suspended…»[10].

Lo cual fue interpretado por algunos como que la empresa estaba amenazando con el cierre del servicio en territorio de la UE de no darse solución a los problemas de transferencia y procesados de los datos de los usuarios a Estados Unidos.

De hecho, en ámbitos estratégicos estadounidenses se destaca el carácter de freno de esta regulación: «Regulations such as the European Union's GDPR have already shown to have adverse effects on free speech, consumer choice, and even scientific research. Further, experts have noted that the GDPR does little to protect privacy and instead focuses almost exclusively on its stated goal of data protection.»[11].

Recientemente se ha producido un hecho relevante en Francia por la Commission Nationale de l'Informatique et des Libertés (CNIL)[12], que ha requerido a una empresa que eliminara de su página web toda referencia al servicio que tenía instalado para llevar a cabo el análisis estadístico de los accesos a su página. Un usuario denunciaba que sus datos habían sido transferidos fuera de la UE, en concreto a EE. UU.; y que, por tanto, se había vulnerado el RGPD.

Incluso los datos anonimizados pueden constituir una vía lateral para la obtención de datos por terceros. Dados los episodios previos en los que operaciones militares se veían

---

[10] KUNDALIYA dev. *Meta threatens (again) to shutter Facebook and Instagram in Europe*. Disponible en: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf

[11] Alexander Kersten y Isaac A. Robinson. Data Protection or Data Utility? Disponible en: https://www.csis.org/analysis/data-protection-or-data-utility

[12] Disponible en: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

amenazadas por la numerosa información que los teléfonos móviles distribuyen de forma a veces incluso inconsciente para sus usuarios, se han adaptado las TTP para evitar estos riesgos. Sin embargo, con el reciente avance de las tropas rusas volvía a producirse un hecho reseñable cuando estudiantes de un instituto de EE. UU. detectaron la irregularidad que se estaba produciendo en el tráfico de las carreteras cercanas a la frontera ucraniana a horas intempestivas. A las 3:15 de la madrugada aparecía en el navegador de sus dispositivos la alerta de embotellamientos en estas carreteras. No habían sido los dispositivos móviles de los propios soldados los que habían dado lugar a esta situación, sino los dispositivos de la población que había visto frenados sus desplazamientos por las barreras que cerraban las vías para el paso de la caravana de vehículos acercándose a la frontera. Tanto los móviles de los conductores y pasajeros como los propios navegadores de los coches estaban remitiendo información a servidores mucho más allá de las fronteras del país que sistemas automatizados estaban interpretando como un atasco[13].

No es la primera vez que el servicio de Google Maps adquiere tintes estratégicos porque, como empresa proveedora de información cartográfica, representa mapas y estos son pizarras en blanco que pueden transmitir muchos mensajes. De hecho, las fronteras recogidas en estos mapas, en ocasiones trascienden la mera geografía y son fruto, tanto su trazado como el tipo de línea utilizado para dibujarlas, del reflejo de la postura de la compañía respecto a ciertos conflictos territoriales.

En el conflicto de Crimea en 2014, Google Maps proporcionaba un mapa diferente según la página web desde la que se cargase el mapa. Accediendo al domino .ru, aparecía una frontera entre la península y el continente, esta frontera desaparecía accediendo al dominio ucraniano, .ua, mientras que, al acceder a la página internacional, .com, se mostraba una frontera discontinua indicativa de la disputa sobre ella[14].

[13] Rachel LermanOn Google Maps, tracking the invasion of Ukraine. Disponible en: https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/
[14] Google Maps Russia claims Crimea for the federation. Disponible en: https://www.theguardian.com/technology/2014/apr/22/google-maps-russia-crimea-federation

Conclusiones

Desde las decisiones del día a día a las estratégicas se están sometiendo a un proceso en el que la incorporación de datos externos cada vez es más necesaria. Es así porque estos datos proporcionan ventajas, porque son útiles, lo que justifica la implantación y los costes necesarios para conseguirlos. Las empresas son especialmente conscientes de ello y, en la actualidad, es muy complicado interactuar de forma anónima en Internet.

Los datos personales son una propiedad privada y, al igual que la tangible, también pasan a ser objeto de protección por la legislación. Son muy diversas las aproximaciones que se pueden adoptar para establecer esta protección, de acuerdo con unos criterios que difieren considerablemente en función de los principios que rigen la labor de los legisladores. Diferentes actores han creado normativa a este respecto que debe encajar la seguridad, la privacidad, la defensa de los intereses económicos y otros principios en línea con sus legislaciones correspondientes. Surgen así contrastes que dan lugar a limitaciones al libre flujo de los datos tanto a la hora de exportarlos como para conservarlos.

Los Estados deben tomar una decisión sobre una materia prima etérea cuyo uso se encuentra en plena ebullición. Puede exportarse para que otros actores expriman el valor creciente que está desarrollando o tomar las medidas para que esa materia prima, los datos, contribuyan al crecimiento local con los incrementos de productividad que su explotación en la industria 4.0 promete y dando lugar a un gran número de puestos de trabajo de alta cualificación en muchos casos.

En paralelo con los intereses económicos, también se debe considerar la cuestión de la privacidad y las libertades de los ciudadanos. En el caso de la Unión Europea, donde la GDPR persigue estos objetivos con medidas restrictivas dirigidas al respeto de estos derechos considerados fundamentales en su tratado fundacional, son muchos los desafíos que están surgiendo ante el modelo actual en el que actores que no responden a estos principios en su totalidad son los principales proveedores de servicios, a la vez que los más interesados en acceder a la información de los ciudadanos.

El dilema entre la protección de datos y el negocio gana intensidad y en esta batalla se está recurriendo a poner sobre la mesa factores directamente relacionados con la seguridad. Así, leyes que facilitan el acceso a la información distribuida fuera de las jurisdicciones nacionales, perteneciente a ciudadanos también fuera de las fronteras del

emisor de la legislación, se justifican con medidas como la lucha contra el terrorismo, la pederastia y la delincuencia. También se utilizan argumentos como las limitaciones al desarrollo tecnológico y al crecimiento que las medidas protectoras de otros Estados suponen para los intereses generales, infravalorando la importancia de estas legislaciones cuyo objetivo es la defensa de los derechos fundamentales de los ciudadanos.

En paralelo se produce una ironía cuando uno de los sectores críticos con las medidas protectoras se posiciona también en una postura de crítica velada a la acción legislativa en otros Estados donde la privacidad del ciudadano se ha visto muy comprometida en pos del rápido crecimiento tecnológico posibilitado por un acceso expedito a la información personal de sus ciudadanos, y que, a su vez, impone serias limitaciones a la incursión en este mercado de entidades extranjeras que pretendan acceder a la materia prima o remitirla más allá de sus fronteras.

Los problemas y ejemplos específicos de situaciones donde la utilización de datos puede afectar a la seguridad nacional deberían servir de referencia a la hora de determinar la importancia con la que debe abordarse la correcta gestión de la información generada por la población de un Estado. Se trata de ejemplos que ya se están produciendo en la actualidad y que serán más numerosos con la creciente aparición de servicios que puedan verse afectados por la naturaleza y calidad de los datos.

Las fronteras físicas suponen barreras para la utilización de los datos de los ciudadanos ante las incompatibilidades de las normativas de los diferentes Estados, aunque no debe olvidarse que, además de las fronteras físicas que surgen principalmente de la legislación, existe otro conjunto de fronteras definidas en este caso por los ciudadanos dictadas por los principios éticos y morales a los que el tratamiento de la información debe someterse.

*David Ramírez Morán**
Analista del IEEE
@DaRamMor