¿De qué me sirve pagar usando la cara o la mano? Pros y contras de este uso de datos

12/10/2020

A raíz de que Amazon haya dicho que quiere que en algunas de sus tiendas en Estados Unidos se pueda pagar usando solo la mano, nos habéis preguntado **hasta qué punto es seguro hacerlo, además de si es útil.** Por ejemplo, en Madrid hay un proyecto en pausa ahora mismo para que podamos pagar con nuestra cara en los autobuses urbanos. Os explicamos **qué tiene de bueno y de malo dar ese tipo de datos** para hacer pagos.

Los datos biométricos son más sensibles que otros como tu nombre o tu dirección

El uso de datos biométricos como la palma de nuestra mano o los rasgos faciales tiene aplicada **una capa de protección extra en el Reglamento General de Protección de Datos (RGPD).** Es decir, que si se van a usar, se tiene que hacer una revisión muy precisa sobre **si el fin es proporcional**: ¿tiene sentido que me pidan mi huella dactilar para algo o podría hacerse mejor de otra manera?

Para usar esta información, tú como cliente tienes que consentir que una empresa como Amazon o el propio consorcio de transportes de Madrid use tus datos **para los fines que ellos te marcan.** La cuestión es: ¿aunque les dieras tu consentimiento, querrías que se trataran unos datos tan sensibles simplemente para pagar?

Todo depende de cuánto te fíes de la empresa a quien vas a cederlos, **ya que tienes que tener en cuenta que es la que los va a tratar**. “Un problema de los sistemas biométricos es el almacenamiento de las características físicas, los patrones biométricos a identificar. El problema también se da en otros sistemas no biométricos, por ejemplo las contraseñas”, explica a *Maldita Tecnología* Andrés Marín, profesor de Ciberseguridad en la Universidad Carlos III de Madrid y maldito que nos ha prestado sus superpoderes.

“También se debe tener en cuenta, que pese a que las empresas que manejan estos datos (principalmente por control de accesos) tienen unos estándares de seguridad especiales para ellos, su precio en el mercado negro es muy alto, por lo que **en los ataques a empresas, son un objetivo prioritario**”, nos explica otro maldito, Jorge Francos, consultor y analista de sistemas.

¿Qué hay del uso de un dato biométrico en sí? ¿Es seguro?

Francos asegura que “para la operación en sí” **son más seguros que otro tipo de datos porque son únicos para cada persona**. Eso sí, esa es un **arma de doble filo**: si los datos son robados o suplantados “quedarían inservibles porque no se pueden cancelar y crear uno nuevo como si nos clonaran la tarjeta de crédito”.

Seguro que alguna vez habréis visto una película de espías en la que para acceder a una cámara subterránea de máxima seguridad hace falta una huella dactilar concreta o incluso un escáner de un iris. **Una vez se consiguen de forma fraudulenta, no hay vuelta atrás**. “Si te roban tus huellas dactilares no las puedes cambiar, y además es difícil enterarte si te las han robado”, añade Marín.

Volviendo a la vida real: ¿cómo podrían llegar a robarnos un dato identificativo tan personal? La Oficina de Seguridad del Internauta (OSI) lo explica en una publicación en su blog: **primero es necesario “tener acceso” a él**. La dificultad varía según el dato biométrico: en el caso de la huella dactilar, nos pasamos el día toqueteando cosas, pero si se necesita la palma de la mano completa se requiere otro tipo de análisis.

Nuestros rasgos faciales, por otro lado, serían incluso más difíciles de suplantar en directo (si vas a pagar en el autobús, por ejemplo). A pesar de ello, ya hay estudios preliminares que concluyen que un *deepfake* puede engañar a sistemas de reconocimiento facial, por lo que **una identificación podría darse por buena aunque estuviese manipulada**.

En definitiva, los datos biométricos son más seguros que otro método de autentificación a la hora de hacer un pago, ya que **robarlos o suplantarlos es mucho más difícil que acceder a una tarjeta de crédito**. Aun así, hay que tener en cuenta dos factores importantes: si alguien se hace con ellos, nuestra seguridad estará mucho más comprometida porque no hay manera de sustituirlos o desvincularlos de nuestra identidad. Y segundo, supone **confiar totalmente en que la empresa que usa tus datos biométricos** solo los va a usar para el fin que te dicen, ya que supone darle acceso a otra intermediaria a una información muy sensible sobre ti.

https://maldita.es/malditatecnologia/2020/10/12/pagar-cara-mano-pros-y-contras-uso-datos/

No, las empresas no pueden utilizar datos del censo para contactarnos (y se enfrentan a una multa si lo hacen)

09/11/2020

Nos habéis preguntado si esto es posible y la respuesta es que no. Por muchas razones, pero la principal es que **en el censo no aparece nuestro número de teléfono** y que ninguna empresa puede acceder a esa clase de datos para hacer una campaña comercial **sin enfrentarse a una sanción**. Además, es algo que como usuarios, podéis denunciar.

El censo es un fichero público que recopila información sobre la población que puede votar. Aparte de nuestro nombre completo y nuestro DNI, incluye información sobre **el domicilio y la provincia en la que residimos**, en la que hemos nacido y también sobre **nuestro grado de escolaridad o nuestro sexo**. No incluye nuestro número de teléfono.

En otras ocasiones se ha explotado el censo para vender datos personales

Eso sí, no es inaudito que alguien se haya **aprovechado del censo para utilizar datos de forma fraudulenta**. En 2011, fue muy sonado el caso de un hombre llamado José Vicente Lucas, que se lucró vendiendo por poco más de 200 euros información personal de alrededor de 35 millones de electores. Distribuía los ficheros a través de una página web llamada “saberlotodo.com”, a la que la Agencia Española de Protección de Datos (AEPD) multó en varias ocasiones. Especialmente, porque no cesaba la actividad.

Cualquier empresa o persona individual a la que se le ocurriese utilizar los datos del censo para venderlos a compañías o simplemente distribuirlos, **se enfrentaría a una multa considerable en caso de ser denunciada**. Pero esto no sólo aplica al censo, sino a la comunicación de datos personales a terceros en general.

Las empresas están obligadas a decir de dónde han sacado nuestros datos

“La ley te obliga cuando llamas a cualquiera a decir **de dónde han sacado tu número de teléfono si no los has obtenido directamente del usuario**. Normalmente, el teleoperador que te asalta estaría obligado a decir de dónde ha sacado tu dato: si de una tarjeta de afiliación, de un registro en una promoción, etc.”, explica a *Maldita Tecnología*, Jorge García Herrero, abogado especializado en protección de datos en el Grupo Secuoya.

Así lo dicta el artículo 14 del Reglamento General de Protección de Datos (RGPD): cuando los datos no se han obtenido directamente a través del interesado deben explicar entre otras cosas **“la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público”**.

¿Qué pasa? Que esto no ocurre nunca, en parte porque no nos conocemos al dedillo las normas que tienen que seguir las empresas en materia de protección de datos y a qué tenemos derecho como consumidores.

Es más, si tienes la certeza de que no has entregado tus datos a la empresa que te llama ni son capaces de explicarte con exactitud cómo los han conseguido, puedes interponer una denuncia ante la AEPD, según nos explica García Herrero.

Los *data brokers*: empresas que recogen, empaquetan y venden nuestros datos personales

También está el hecho de que a día de hoy, **el mercado de compra-venta de datos personales es una verdadera jungla**. Ya no solo intervienen los datos que se obtienen a partir de las aplicaciones que usamos o que sacan las tecnológicas y las redes sociales, sino que hay **empresas de márketing dedicadas especialmente a recabar datos personales** de fuentes públicas, registros, transacciones online, nuestra navegación… A estas compañías se las llama *data brokers*.

García Herrero asegura que a la hora de hacer campañas comerciales, muchas empresas recogen y compran datos de donde pillan, incluidas estas compañías dedicadas a empaquetar datos personales y venderlas a otras.“Que un dato personal se haya hecho manifiestamente público por una persona, **no quiere decir que cualquiera otro titular, pueda captarlo y utilizarlo** para lo que le dé la gana”, afirma el abogado.

Nos habéis nombrado una empresa concreta que ha dicho obtener los datos de esta manera: Securitas Direct. Hemos contactado a la compañía, que nos asegura que desde su departamento de contacto realizan llamadas a personas que han dejado sus datos en su página web o que obtienen gracias a las diferentes campañas que realizan.

Como ya os hemos comentado, muchas empresas obtienen nuestros datos de contacto a través de *data brokers* o de campañas anteriores (ya que en algunas ocasiones guardan los datos durante años). Sin embargo, **también os animamos a ser especialmente cuidadosos con dónde introducís vuestros datos de contacto**: en promociones, en registros para ofertas, en formularios en páginas web… En los Términos y Condiciones **muchas veces avisan de que esos datos se comparten con la empresa X** y no nos habríamos dado ni cuenta.

https://maldita.es/malditatecnologia/2020/11/09/empresas-no-pueden-utilizar-datos-censo-para-llamar-multa/

Malditos datos: Cómo puedo saber qué información tienen las empresas sobre mí

24/08/2020

Esta es una pregunta que en alguna ocasión nos han hecho los malditos y las malditas: mucho hablar de datos personales y de cómo los extraen a partir de aplicaciones o redes sociales pero, **¿cómo sé qué datos tienen exactamente las empresas sobre mi?**

Lo primero es que no hay una respuesta directa a esa pregunta, ya que no es del todo posible saber **cuántas empresas en todo el mundo tienen datos sobre nosotros o cuáles son** esos datos exactamente. Nos explicamos: cuando haces uso de una aplicación o un servicio en Internet, normalmente aceptas que la entidad que te presta ese servicio **pueda compartir ciertos datos** con socios, con otras compañías que intervienen a la hora de dártelo, con empresas intermediarias como los data brokers, etc.

Sí que **tenemos derecho a saber qué información sobre mí tiene esa empresa concreta** a la que yo le he pedido el servicio, por ejemplo, el banco Santander a la hora de abrirme una cuenta o Facebook cuando uso la red social. Tenemos derecho incluso a saber con qué información cuentan sobre nosotros los **partidos políticos**, que **también manejan nuestros datos personales.** ¿Cómo? A través del llamado **"derecho de acceso"**.

Un derecho fundamental todavía muy desconocido: ¿cómo funciona?

Para explicaros todo sobre el derecho de acceso nos ayudan desde MyDataMood, una plataforma dedicada expresamente a facilitar la solicitud de este y otros derechos relacionados con la protección de datos: oponerse a que usen nuestros datos, pedir que los rectifiquen si son erróneos, etc.

Sabina Guaylupo, jefa de Producto en MyDataMood, nos explica que el derecho de acceso es **uno de los derechos fundamentales** reconocido en el art.8.2 de la Carta de los Derechos Fundamentales de la Unión Europea: *"Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación"*. Guaylupo afirma que este es un derecho **independiente**, es decir, que no tienes que solicitar el de acceso antes para pedir cualquiera de los otros que tienen que ver con tus datos.

También lo contempla el Reglamento General de Protección de Datos europeo (art. 15) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (art. 13), pero **su uso apenas es conocido para la sociedad**.

Organismos públicos o empresas que manejan datos sensibles o de forma masiva, entre otros, deben contar sí o sí con un **Delegado de Protección de Datos (DPO)**, que es la figura encargada de asegurarse que se vela por la protección de los datos personales y que **gestiona las peticiones de los usuarios**, y es a ella a quien hay que dirigirse.

Normalmente, los datos de contacto del DPO **vienen recogidos en las políticas de privacidad** de dichas compañías, pero si no cuentan con uno debe haber una dirección de

correo genérica a la que acudir. Para ello, debes acudir al apartado del documento que ponga "Responsable del tratamiento":

¿Qué podemos pedirle a la empresa que nos de?

Según el RGPD, podemos pedirle unas cuantas cosas a una empresa: **para qué** usan los datos, **durante cuánto tiempo** lo hacen, **qué destinatarios los reciben**, si los trata un programa automatizado o **si elaboran perfiles con ellos** (y las consecuencias que eso puede tener).

"A lo primero a lo que el usuario tiene derecho es a saber **si se están tratando o no** datos personales que le conciernen. En caso afirmativo, tiene derecho a recibir una **copia de los mismos.** Esto significa que no es suficiente con que nos digan que tienen los datos necesarios para llevar a cabo el servicio o realizar un contrato, si no que nos tienen que dar copia", asegura Guaylupo.

Sí, una empresa de comida a domicilio nos tendrá que mandar el listado de todos nuestros pedidos, no solo decirnos que los tienen apuntados por ahí.

¿Qué más cosas se pueden saber gracias al derecho de acceso? Guaylupo nos da algunas indicaciones más: **qué categorias de datos se tratan**, si son identificativos, si son de salud, etc. ("quizás algunos se los hemos proporcionado nosotros, pero otros no y no podemos ni imaginar que los tienen", avisa). También **se puede preguntar por el origen** si sé que no los he dado yo directamente o **si se transfieren a un tercer país u organización internacional** y en qué condiciones.

Para terminar, una de las cosas más importantes que podemos pedir: si someten a nuestros datos **a la elaboración de perfiles y a decisiones automatizadas:** "Si están aplicando algoritmos o se están elaborando perfiles basados en los datos de las personas hay que explicar cómo funciona ese algoritmo, la lógica que usa, y cuales son las reglas que se aplican", explica Guaylupo.

Por eso es tan importante hacer uso del derecho de acceso: debería ser una herramienta para entender por qué nuestra operadora nos ofrece una oferta u otra o por qué un banco me concede o niega un préstamo.

Haz uso de tu derecho de acceso

Una vez tenemos localizada la dirección de correo a la que tenemos que enviar nuestra solicitud, debemos saber qué mandar específicamente. Siempre te van a pedir unos datos concretos como **nombre y una imagen de tu DNI** u otro documento identificativo, así que para ahorrar pasos puedes adjuntarlo en el primer correo que mandes.

Aquí te dejamos **un modelo de correo electrónico** que puedes mandar al DPO de una empresa **para solicitar tu derecho de acceso**. Recuerda luego **seguir pendiente de ese hilo de correos**, porque **con mandarlo solamente no basta**, es más que seguro que el proceso requiera **algún paso adicional** que te pedirá cada empresa u organización (por ejemplo, confirmar que quieres solicitar la copia):

D./Dña. _____, mayor de edad, con domicilio en la calle _____, Código Postal _____, con DNI _____, del que acompaña fotocopia, y correo electrónico _____ *(el que tengas asociado a dicho servicio)*_____ por medio del presente escrito solicita ejercer su derecho de acceso, de conformidad con el **artículo 15 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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**.

SOLICITA:

1) Que se le facilite el derecho de acceso al tratamiento de sus datos personales en el plazo máximo de **un mes** a contar desde la recepción de esta solicitud.

2) Que si la solicitud del derecho de acceso fuese estimada, se me facilite una copia de los datos personales objeto de tratamiento.

3) Que esta información comprenda de modo legible e inteligible los datos que sobre mi persona están incluidos en sus tratamientos, así como la siguiente información: los fines de dichos tratamientos; los destinatarios o las categorías de destinatarios a los que se comunicaron; el plazo previsto de conservación; la existencia de decisiones automatizadas y transferencias internacionales de datos.

Atentamente,

https://maldita.es/malditatecnologia/2020/08/24/malditos-datos-como-puedo-saber-que-informacion-tienen-las-empresas-sobre-mi/

Malditos Datos (II): Cómo evito que las empresas utilicen mis datos sin mi consentimiento

18/11/2020

Tras explicaros cómo podemos saber qué información tienen guardada las empresas sobre nosotros a través del derecho de acceso, toca hablar de **cómo podemos oponernos a qué usen esos datos para según qué cosas**. Ojo que no es algo que podamos pedir bajo cualquier supuesto, sino que está condicionado a que **hayamos dado permiso o no** a esas organizaciones y empresas para usar los datos (aunque sea sin querer).

Pero vamos por pasos: el **derecho de oposición** está incluido en la lista de derechos que podemos ejercer si hablamos de nuestros datos personales y sirve para **instar a las entidades que estén utilizando esa información a dejar de hacerlo**, tal y como nos explica **Sabina Guaylupo**, abogada y jefa de Producto en MyDataMood, una plataforma dedicada expresamente a facilitar la solicitud de este y otros derechos.

Que puedas hacer uso de él o no depende de dos supuestos: que la empresa, el partido o la organización a la que vas a pedir esta oposición **esté usando tus datos de forma lícita y con tu consentimiento** o que los estén usando con **fines comerciales**. Os lo explicamos más a fondo.

Qué es el consentimiento y por qué es importante

El consentimiento es **la palabra favorita de las empresas que usan tus datos para determinado fin**. Muchas veces es en lo que se amparan para hacer lo que sea con tu información: **que tú les has dado permiso para ello** ya sea a través de una casillita que marcas haciendo clic, aceptando algunas cookies, incluyéndolo en una Política de Privacidad, etc.

Si no cuentan con la bala del consentimiento, seguramente estén basándose en uno de los tres supuestos bajo los cuales pueden tratar tus datos para sus propios intereses y que nos enumera Guaylupo: el **"interés púbico"**, el ejercicio de **"poderes públicos"** que se atribuyen a quien usa los datos o por razones de **"interés legítimo".**

Algunos cuadros que nos animan a **aceptar la instalación de cookies** son un ejemplo. Si eres de esas personas que entran a configurar las cookies para no aceptarlas todas, verás que a veces son dos las casillas que hay que desmarcar: **la del consentimiento y la del interés legítimo**. Desactivar este último al final es una manera de ejercer el derecho de oposición.

Alto el carro: ¿y cómo distinguimos a qué se está acogiendo una empresa o una organización para tratar nuestros datos, entonces? Nos contesta Guaylupo: "Podemos **revisar las políticas de privacidad de las páginas web**, y veremos cómo al registrarnos, para determinados tratamientos como ceder nuestros datos a terceros nos piden el consentimiento".

Sin embargo, para **otros tratamientos como enviarnos comunicaciones comerciales o incluso para tratar nuestros datos personales para perfilarnos**, "no nos piden el consentimiento si no que se amparan en su 'interés legítimo'", añade esta especialista.

No nos podemos meter en este artículo en **cuándo se puede amparar una empresa en el interés legítimo y cuando no**, ya que tendríamos que dejar lo del derecho de oposición para otro día **debido a lo amplio que es el concepto**: "Baste decir que aún estamos en el camino de encontrar el equilibrio entre el buen uso y el abuso de esta base de legitimación para poder tratar datos personales", explica Guaylupo.

Existen muchas triquiñuelas para conseguir que hagamos clic en cosas que realmente no queremos, también para conseguir que aceptemos por ejemplo el envío de publicidad sin darnos cuenta. Por eso uno de los principales consejos de la Agencia Española de Protección de Datos (AEPD) es que **estemos atentos cuando navegamos por Internet para comprobar qué estamos firmando** y qué nos están pidiendo.

Así que cuidadín, porque dar permiso a una empresa para que use tus datos también puede implicar hacerlo aceptando una Política de Privacidad o unos Términos y Condiciones que no nos hemos leído al pulsar "Aceptar".

El otro supuesto: si quiero dejar que usen mis datos con fines de mercadotecnia

Esto alude a los datos que se usan con un objetivo comercial: para hacer márketing y comercializar productos. El derecho de oposición también nos permite exigir a las empresas que **no usen nuestros datos para enviarnos publicidad** si no hemos dado nuestro consentimiento.

Una manera muy extendida de hacerlo es a través de la Lista Robinson, de la cual os hemos hablado en otro artículo. Es un fichero de exclusión publicitaria al que podemos apuntarnos **para no recibir llamadas o mensajes de empresas** que quieran vendernos publicidad.

En este supuesto también se incluye la elaboración de perfiles para mandar publicidad. O sea, que las empresas **no usen nuestros datos para generar información sobre lo que nos gusta y lo que no** y mandarnos publicidad afín.

El derecho de oposición y revocar el consentimiento no es lo mismo

Creednos que si os hemos explicado todo el rollo del consentimiento, es por algo: dependiendo de lo que estemos buscando, no vamos a necesitar pasar por el trámite de ejercer nuestro derecho de oposición.

Nos explicamos: si al darle ciertos datos a una empresa **estaba contemplado** que en un futuro pudiesen usarlos para otros cometidos **no hará falta ejercer el derecho de oposición**, aunque el objetivo sea el mismo, oponerte a que usen ciertos datos. Porque en ese momento les diste tu permiso para ello, así que lo que habría que hacer es retirarlo.

¿Cómo? "En la práctica, **bastaría con informar, a través de un email, por ejemplo, al responsable del tratamiento de nuestros datos** de nuestra retirada de consentimiento para que ésta se produjera", explica Guaylupo.

Os ponemos un ejemplo que igual recordáis: en noviembre de 2019, se supo que el Instituto Nacional de Estadística iba a utilizar **datos de localización anonimizados de las operadoras para conducir un estudio de movilidad**. Ese tratamiento de nuestros datos anonimizados **estaba contemplado en las políticas de privacidad** de las compañías, así que lo que nos pedían para dejar de formar parte del estudio era comunicar mediante email la retirada del consentimiento o desactivarlo en la app.

Haz uso de tu derecho de oposición

Como el resto de derechos relacionados con la protección de datos, la solicitud de oposición **la podemos presentar directamente nosotros, como interesados, o a través de un representante**. Así es como lo hacen en MyDataMood: actúan en calidad de mandatarios para ejercer estos derechos por ti (algo que contempla la legislación actual).

En caso de que prefieras hacer el trámite por tu cuenta, habrá que seguir algunos pasos que ya te contamos con el derecho de acceso, como buscar el correo del Delegado de Protección de Datos (DPD) de la empresa a la que quieres pedir que deje de usar tus datos. **Lo encontrarás en la Política de Privacidad de su página web**.

Una vez lo tengamos, rellenaremos un formulario de la AEPD que adjuntamos en este artículo para mandárselo. Hay dos modelos: el (A) es para el primer supuesto (si la empresa dice que usa tus datos por interés legítimo, por ejemplo) y el (B) para los casos de uso publicitario.

Una vez hayas enviado el formulario junto a una copia de tu DNI, las empresas tienen hasta un mes para confirmar el trámite. En caso de que no lo cumplan, podrás poner una denuncia ante la AEPD.

https://maldita.es/malditatecnologia/2020/11/18/malditos-datos-como-evito-que-empresas-utilicen-datos-sin-consentimiento/

Puntos clave en los que fijarte en las Políticas de Privacidad (aunque lo mejor es leerlas enteras)

23/07/2020

Hay una cosa que te vamos a conceder con las políticas de privacidad y es que son tremendamente largas y tediosas. ¿Sabes qué pasa? Que la mayoría **están hechas así a propósito** para que, o bien no te la leas entera, o no te enteres del todo de lo que te están contando y termines **aceptando cosas que en realidad no querrías aceptar**.

A eso se suma que antes de hacer click en “Aceptar” no sólo nos piden que aprobemos la Política de Privacidad, sino también los Términos de Uso o Términos de Condiciones. Otro **documento legal larguísimo que no tenemos tiempo para leer**, algo que sí se ha hecho en experimentos para concluir que son incomprensibles.

Imagina que cada vez que vas a descargar una aplicación, darte de alta en una red social, comprar un billete de bus o avión, hacer una compra online, suscribirte a un periódico o lo que sea, tuvieras que leer **entre media y una hora (¡una hora!) las condiciones**. Al final no lo haces y está demostrado que es por **esa complejidad que presentan**: leer las condiciones de Microsoft, por ejemplo, nos llevaría el mismo tiempo que leer Macbeth, de Shakespeare.

Los Términos y Condiciones se adaptan un poco a la función de cada plataforma, aunque comparten aspectos básicos como **una serie de normas que tienes que seguir** para usarlas: por ejemplo, las licencias que les das a las redes sociales al subir contenido (para que ellas luego lo distribuyan como les parezca).

Eso sí, las Políticas de Privacidad suelen ser muy parecidas entre ellas (a veces calcadas porque las empresas literalmente copian modelos de Internet y sólo cambian el nombre) y **deben incluir una serie de cosas básicas sobre lo que recogen sobre ti y lo que hacen con esa información**. Por eso, podemos darte algunas pistas para que vayas a tiro hecho a la hora de leer una y sepas **en qué tienes que fijarte** sí o sí.

Hemos preguntado a **abogados especializados en protección de datos** y estos son las claves que nos han dado:

1. ¿Para qué los quieren?

El meollo de la cuestión. La mayoría de estos documentos suelen hablar de esto en una lista de puntos donde cuentan cada uno de los supuestos. La mayoría te hablarán de “prestarte el servicio”, “cumplir con la ley”, “ofrecerte publicidad” y “asegurarse de que todo funciona y mantener la seguridad”. ¿Hay alguna que no cuadra con el servicio que estás usando, como que vayan a recogerlos para “inferir” nuestros intereses para ofrecernos algo? Pues ojo.

2. ¿Cuánto tiempo los van a guardar?

Aquí viene uno de los puntos conflictivos de la mayoría de las políticas, porque muchas empresas se escaquean de decir cuánto tiempo lo harán aludiendo a motivos comerciales o judiciales. Es cierto que tienen que guardar los datos durante un tiempo por si acaso los exige un juez, pero cuando hablan de usarlos mientras sea necesario para prestar los servicios, por ejemplo… ¿Eso cuánto es? ¿Un mes, un año, tres años?

Algunas compañías siguen usando la información que recopilan de nosotros (aunque sea de manera agregada) para fines publicitarios o estadísticos, pero tampoco sabemos a ciencia cierta cuánto, así que si no lo especifican, no nos gusta. Y si tiran de una oración complicada y genérica de tres líneas para justificarlo, tampoco. Así que no te cortes y pregunta si no estás satisfecho/a con la respuesta.

3. ¿Con quién los van a compartir?

Otro punto delicado al que hay que acudir obligatoriamente. Aquí puede que te encuentres frases del estilo: “No compartiremos tus datos nunca con terceros”, pero es difícil que esto sea tan estricto. Si una aplicación pertenece a una empresa que tiene socios o, por ejemplo, tiene opción de acceso con Google y Facebook, hay datos que se pueden compartir.

Con fines publicitarios la mayoría de empresas de redes sociales, juegos, páginas de viaje, tiendas online, etc. van a compartir información, porque lo que buscan es hacerte llegar la publicidad que te lleven hasta ellos. Cuanto más claro te digan con quién van a compartirlos, mejor, más informada será tu decisión de usar el servicio.

Como os decíamos, las Políticas de Privacidad **están diseñadas para aburrirnos hasta la saciedad y confundirnos**. ¿Que una es relativamente corta o explicada en un esquema fácil de entender? Las políticas de privacidad no van al peso: si te explica el funcionamiento del servicio y lo que hace con tus datos **de forma fácil y sencilla** es un sinónimo de que los desarrolladores se lo han tomado en serio, saben que no quieres leerte El Quijote y te han contado lo que tienes que saber sin intentar que desesperes.

https://maldita.es/malditatecnologia/2020/09/28/puntos-clave-politicas-de-privacidad/

Qué hacer ante la difusión de imágenes íntimas o de carácter sexual en Internet

24/07/2020

En otras ocasiones os hemos contado qué hacer si alguien ha distribuido por redes sociales un contenido subido por mí y se ha hecho viral y también cuándo están obligadas a retirar algo si lo pide su autor, pero este caso concreto entra en un saco diferente, al menos en España. Si ves o te enteras de que alguien ha subido **una foto o un vídeo íntimo de ti o con carácter sexual**, no tienes que lidiar con la red social en cuestión si no quieres, sino que puedes acudir a la **Agencia Española de Protección de Datos (AEPD)**.

En 2019, la AEPD abrió lo que llamó un "Canal prioritario" para solicitar la retirada exprés y urgente de material "sensible". Es decir, fotos y vídeos de carácter sexual **difundidos sin la autorización de la persona** que aparecía en las imágenes o que muestran agresiones.

La idea es que la Agencia **actúa de intermediaria pidiéndole directamente a las operadoras y proveedores de servicios en Internet** (Facebook, Google o Twitter, por ejemplo) la retirada urgente del contenido, de modo que el proceso no se alargue eternamente.

¿Cómo funciona y qué tengo que aportar?

Se puede acceder al canal a través de este enlace, donde te dan la opción de hacer el proceso de forma electrónica o con soporte en papel. En el primer caso, necesitaremos tener **firma electrónica (Cl@ve pin)**. Se deben describir con el mayor grado de detalle las **circunstancias en las que se han difundido sin consentimiento las imágenes**: ¿es víctima de violencia de género? ¿Se la ha discriminado por su orientación sexual, su procedencia o porque tiene alguna discapacidad? ¿Es menor?

En el caso de ser menor de 14 años, es el padre o madre quien tiene que hacer la solicitud, pero antes, la AEPD tiene un apartado específico para que **los menores se pongan en contacto con ella**: se accede en este enlace.

También se deben **adjuntar direcciones web** por las que se está difundiendo (copiar y pegar el enlace de la página web) o **identificar a las personas que lo están compartiendo** en sus redes sociales. Además, hay que especificar si ya se ha tratado de denunciar por otras vías, por ejemplo ante la policía, o si has tratado de ponerte en contacto antes con la red social o plataforma en cuestión.

Si tienes documentación que crees que podría ser relevante, por ejemplo **capturas del servicio por el que se están difundiendo las imágenes** o incluso del dispositivo en cuestión, también se pueden adjuntar.

¿Cómo sigue el procedimiento?

Una vez hecho todo esto, la Agencia atenderá la petición con prioridad y después determinará si ordena a las plataformas involucradas **que retiren el contenido**. Además, si

tienen indicios de que se haya producido un delito, lo comunican a la Fiscalía. Llegados a este punto, se comunicarían contigo, pero para ir siguiendo la denuncia a través del "Canal prioritario" hay que darse de alta en la "carpeta ciudadana (también con Cl@ve).

Una cosa importante de este mecanismo es que **no tiene que ser necesariamente la víctima la que haga la denuncia**, sino que puede hacerlo cualquier persona a la que le llegue una foto o vídeo de estas características y tenga constancia de que **se ha difundido sin permiso.**

La AEPD también enumera una lista de enlaces a los cuáles podemos acceder para hacer una petición similar a **las principales plataformas y redes sociales**, en caso de que queramos probar por esa vía: Bing, Blogger, Dailymotion, Facebook, Flickr, Google, Instagram, Snapchat, Tumblr, Twitter, WordPress, Youtube.

https://maldita.es/malditatecnologia/2020/10/03/difusion-imagenes-intimas-caracter-sexual-internet/

Cómo denunciar una infracción relacionada con mis datos personales a la Agencia Española de Protección de Datos

06/08/2020

Hace poco, os contamos cómo podéis denunciar ante la **Agencia Española de Protección de Datos (AEPD)** la difusión de imágenes íntimas de una persona o con carácter sexual en Internet. Ahora, nos habéis preguntado directamente **cómo hacer una denuncia ante este organismo** para infracciones relacionadas con nuestros datos personales.

Lo primero es lo primero: ¿qué se puede denunciar ante la AEPD?

Únicamente cuestiones que estén **relacionadas con nuestros datos personales**, no con nuestro derecho al honor o a la intimidad, por ejemplo, ya que esos casos se tramitan directamente ante la Justicia.

Un ejemplo práctico sería interponer una denuncia porque **alguien ha colgado tus datos, como tu dirección o tu DNI, sin tu consentimiento** en Internet. Otro sería que una empresa usase tus datos para **algo que no estaba contemplado cuando los diste**: por ejemplo, que des tus datos a una discoteca por la COVID-19 y luego te contacte a través de él alguien que no trabaja para una autoridad sanitaria para algo que no tenga relación con el virus.

¿Cuál es el procedimiento?

Para hacerlo a través de Internet, debes acceder al menú "Trámites" y una vez ahí **seleccionar la opción que se ajuste al motivo de tu reclamación**: denunciar que estás recibiendo información comercial de una empresa cuando has pedido que no usen tus datos para ello o que te hayan grabado con una cámara de videovigilancia sin tú saber para qué, por ejemplo.

Recuerda que para hacer trámites de este tipo **online**, necesitarás contar con **alguna forma de autenticación**, como la Cl@ve Pin. Si prefieres presentarlo de forma física (con soporte en papel) deberás hacerlo en una oficina autorizada y junto a una serie de datos que puedes encontrar en este enlace. A través del menú "Trámites" obtendrás el **justificante de tu reclamación**, que deberás presentar junto al resto de información.

A la hora de hacer una denuncia ante la AEPD hay que tener en cuenta que **se deben presentar bastantes documentos** relacionados con ella, sobre todo relativos a la información que **hayamos podido recopilar** sobre la situación que queramos denunciar.

A medida que avancemos en el formulario electrónico (al veremos que no nos piden solo nuestros datos, sino información en detalle de lo ocurrido. **Todas las pruebas que tengas disponibles sobre el caso deberán ser presentadas** (documentación, imágenes, mensajes, etc.), especialmente si hemos tenido comunicaciones con la empresa o entidad con la que hemos tenido problemas por un uso indebido de nuestros datos.

Por eso, si por ejemplo acudes a la AEPD porque una compañía telefónica no para de llamarte cuando ya has pedido que no lo hagan, **te pedirán que antes trates de ejercer tus derechos** relacionados con los datos personales: de acceso, rectificación, oposición o cancelación. En este caso, especialmente el último tiene que ver, ya que puedes pedir a las empresas que borren y dejen de utilizar tus datos. En este enlace, la Agencia da más información sobre ellos y cómo ejercitarlos.

Con qué no puede ayudarte la AEPD

Por último pero no menos importante, te dejamos este enlace en el que puedes ver todo aquello con lo que la AEPD **no puede ayudarte** (por ejemplo, a pelearte con tu operadora porque no ha respetado el contrato que firmasteis).

https://maldita.es/malditatecnologia/2020/08/06/denunciar-infraccion-datos-personales/

Lista Robinson: cómo evitar las llamadas y mensajes de futuras campañas publicitarias

14/09/2020

Puede que muchos de vosotros hayáis oído hablar de la **Lista Robinson**, a la que te puedes apuntar para **evitar que las operadoras y otras empresas te bombardeen con llamadas y mensajes para que compres sus productos**. Y si no la conocías, ya estás tardando en finiquitar este artículo para enterarte de qué va la cosa. Ahora bien, ¿por qué están las empresas obligadas a excluir de sus campañas comerciales a las personas que aparecen ahí apuntadas?

La lista Robinson: un fichero para ejercer el "derecho de oposición"

La Lista Robinson lleva funcionando desde 1993, aunque en ese momento se utilizaba para que la ciudadanía pudiera **oponerse a que le enviaran publicidad por correo postal** y no por Internet. Según cuenta a *Maldita Tecnología* Emilio Suárez, responsable jurídico de Adigital, la asociación que la fundó y dirige desde entonces, el paso a lo digital se hizo cuando entró en vigor la Ley Orgánica de Protección de Datos de 1999 y su reglamento de desarrollo en 2007.

Cuando se disparó el uso de Internet y las empresas aprovecharon para crear nuevas estrategias comerciales, se buscaron maneras de hacer más accesible el derecho a la oposición, que nos asegura que una empresa **no utilice los datos personales que tiene sobre nosotros para un determinado fin** si se lo solicitamos.

Para facilitar el ejercicio se creó el concepto de **fichero de exclusión publicitaria**, al que responde la Lista Robinson y que operan en España bajo regulación nacional. No solo para cubrir la publicidad en Internet: la lista hace posible que podamos oponernos a recibir llamadas indeseadas, correos electrónicos, SMS, etc.

Luego entró en vigor el Reglamento General de Protección de Datos (RGPD) europeo y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales y su uso se extendió más aún. A día de hoy hay cerca de **1.200.000 personas inscritas** en ella, según Suárez, aunque no es el único fichero que hay con esta función.

¿Por qué están las empresas obligadas a comprobarla?

Los ficheros de exclusión publicitaria como la Lista Robinson vienen incluidos el artículo 23 de la LOPD, que dice que pueden crearse “sistemas de información” que incluirán “datos imprescindibles para identificar a los afectados” con el objetivo de “enviar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas”.

Las empresas tienen que mirar esta lista si los ciudadanos no han dado su consentimiento para que se les contacte porque **es una forma válida que tienen de ejercer su derecho a la oposición** del uso de datos.

¿Y por qué es Adigital quien tiene que gestionar los datos de la Lista Robinson? La ley también indica que las entidades que manejen ficheros como esta lista deben tener el visto bueno de la Agencia Española de Protección de Datos (la autoridad de control competente), como es el caso de la asociación.

“El sistema de consulta de la Lista Robinson por parte de las empresas fue diseñado para garantizar que **estas nunca tengan acceso a los datos de los ciudadanos inscritos**, al mismo tiempo que nosotros no tenemos acceso a los datos de la empresa”, nos explica Suárez.

Si quieres apuntarte a la Lista Robinson, puedes hacerlo desde este enlace. Ten en cuenta que el efecto **no es inmediato**: si una empresa ya ha iniciado una campaña publicitaria y no estabas apuntado desde antes en el fichero, podrás seguir recibiendo comunicaciones.

https://maldita.es/malditatecnologia/2020/11/18/lista-robinson-evitar-llamadas-mensajes-campanas-publicitarias/

Geolocalización, cámaras térmicas, apps: los más y los menos de las iniciativas tecnológicas contra COVID-19 en cuestión de datos personales

08/05/2020

Durante el confinamiento se han puesto en marcha una serie de iniciativas digitales, desde aplicaciones para móvil a chabots para conversar, y parece que para la desescalada se viene otra ola de propuestas **que se centran en encontrar maneras para atajar los contagios**. Con sus ventajas y sus desventajas: lo primordial es que se desarrollen con la mayor precisión **para que no haya incidentes con los datos personales**. La Agencia Española de Protección de Datos (AEPD) las resume todas en un documento en el que las analiza desde la perspectiva de la protección de datos. ¿Cuáles son sus beneficios y sus riesgos, según este organismo?

Usar la geolocalización de los móviles para analizar el virus en función de cómo se mueve la ciudadanía

Ya sea a través de las **operadoras de telefonía** o de la que se puede extraer de **redes sociales**, la geolocalización se considera un dato que **puede convertirse en una amenaza a la privacidad** de las personas. Especialmente, si se recoge de forma masiva. Y te preguntarás, ¿geolocalización a partir de redes sociales? Sí, la agencia se refiere a la que registra la dirección IP con la que **nos conectamos a Internet**. Lo creas o no, se puede usar para **estimar dónde está la gente**: Facebook y Google lo hacen con fines publicitarios.

El uso de este tipo de localización **presenta más riesgos** debido a que se pudiese enriquecer este dato "con información personal **derivada de la actividad en los perfiles de usuario** o si se toman acciones sobre sus perfiles". La agencia desdeña las condiciones de uso y las políticas de privacidad de las redes sociales a la hora de considerarlas una "base jurídica adecuada" para este tipo de uso. Es decir, que **no son la mejor garantía para mantener segura** la privacidad.

En cuanto a la que se recoge a través de las antenas de telefonía, la AEPD considera que "siempre cabe la posibilidad de una **anonimización incompleta**, una subcontratación poco rigurosa o un **ciberataque** que pusiera en manos de un tercero la localización de los móviles de los usuarios". Pero que eso también estaba en riesgo **aunque no hubiese una pandemia mundial** causada por el coronavirus.

Tal y como nos encontramos ahora, sin embargo, la agencia cree que puede resultar de utilidad a las autoridades (aquí te hablamos del estudio de movilidad planeado por esta causa) para fijarse **dónde puede concentrarse una cantidad de gente considerable** y estudiar el virus en relación. Esta "foto" general puede servir para detectar focos de infección o estimar la saturación de la sanidad de una provincia, pero **no arregla el problema que hay para detectar los contagios**. Ahí es donde entra el 'tracing' de contactos.

Apps de 'contact tracing' o rastreo de contactos que funcionan por bluetooth

El gran tema del momento, que se presenta como **la más respetuosa con la privacidad**, pero a la que la agencia también le saca pegas. Sobre el 'contact tracing' o seguimiento de contactos te hemos hablado a fondo aquí y sobre las concreciones de por qué las apps funcionan con bluetooth, aquí.

Tal y como contamos en esos artículos, la idea es que estas apps sean **complementarias a otras técnicas que pueda introducir Sanidad**, como el rastreo manual. Para que funcionen es necesario que las instale más de la mitad de la población y la AEPD considera que serán realmente útiles cuando **se cuente con personal para atender los casos de infección** que reporten las personas y cuando haya suficientes tests para toda la gente que se detecte a través de una aplicación así.

En cuanto a los riesgos, la agencia resalta que pudiesen hacerse **"mapas de relaciones entre personas"** o que se reidentificara a alguien a raíz de su localización implícita. El riesgo está en que al tratar mi información, no sólo estoy yo en el punto de mira sino todos mis contactos. También **desecha un modelo centralizado** debido a la posibilidad de que "se produjese un abuso de una empresa poco ética" y por el riesgo de un ciberataque.

Apps de autodiagnóstico y control de contagios: colaborativas y oficiales

Lo que caracteriza a este tipo de aplicaciones es que muchas veces surgen de iniciativas ciudadanas o empresas privadas. Y eso, trae sus riesgos. ¿Qué pasa si una aplicación que dice servir a un fin y ser altruista **luego no especifica lo que hace con tus datos**? La agencia señala también que "las prisas conducen a **desarrollos sin garantías para la privacidad**" y hablamos de datos de nuestra salud, que no son moco de pavo. Es información que nos puede hacer mucho daño en un futuro si cae en malas manos, por ejemplo, a la hora de contratar seguros o pedir trabajos.

La supuesta ventaja que tienen estas apps es que **se plantean como una alternativa** para quienes desconfían de las actuaciones de las autoridades, según la AEPD. Ahora bien, ¿es suficiente excusa esa como para confiar datos personales, de salud o de localización a terceros?

En cuanto a las aplicaciones que han dispuesto el Gobierno y las comunidades autónomas para hacerse autoevaluaciones, la principal pega que pone es que **por la "urgencia en ofrecer soluciones" se puedan llegar a relajar los controles** para proteger los datos a la hora de crearlas. Este fue el caso de la aplicación de autodiagnóstico de la Comunidad de Madrid, **Coronamadrid**, que unos días después de su lanzamiento tuvo que modificar su Política de Datos para reforzar la protección de la información que recoge.

Pasaportes de inmunidad para llevar en el móvil

Esta tecnología es algo de lo que todavía no se ha hablado en España, pero sí que se han planteado en Alemania, Italia o incluso Estados Unidos. Imagina **una especie de tarjeta de embarque con un código QR** que pudieses guardar en una app y contuvese información

sobre ti y **si has pasado por la COVID-19 o no**. Luego, al viajar, lo presentarías ante las autoridades para que **te dejen pasar o no** según lo que ponga en ella.

El principal problema que ve la AEPD en ellas es que al depositar información que **nos identifica y que además agrega datos de salud**, es una bomba de relojería. En primer lugar, porque **las pueden hackear o introducir metadatos** que puedan dar más información de la que debieran. Pero luego está lo más importante: todavía no hay evidencias de que al superar la COVID-19 no podamos volver a infectarnos, tal y como cuentan nuestras compañeras de *Maldita Ciencia*, por lo que estos pasaportes no tendrían validez.

En cuanto a sus beneficios, se apoya en informes antiguos de la Organización Mundial de la Salud (OMS) para mencionar que se ha potenciando el desarrollo de aplicaciones de salud móvil para que podamos llevar nuestro historial clínico en el bolsillo siempre. Sus requisitos para que una tecnología así funcionase es que fueran "actualizados, seguros e interoperables" y que solo tuvieran acceso a ellas las autoridades.

Cámaras de infrarrojos para leer la temperatura de la gente en establecimientos

De estas te hemos hablado hace poco en este artículo. En él incluimos las consideraciones de la AEPD, que en este caso concreta que "no se puede tomar un dato de salud de una persona y **tratarlo espontáneamente por cualquier gestor de un lugar público** simplemente porque crea que es lo mejor para sus clientes o usuarios". No parece encontrarle ningún beneficio a esta medida tecnológica a no ser que la autorice el Ministerio de Sanidad.

https://maldita.es/malditatecnologia/2020/05/08/geolocalizacion-camaras-termicas-apps-covid-19-datos-personales/

¿Qué puede hacer una cámara térmica o un control de fiebre en locales y comercios contra el coronavirus y cómo se manejan los datos que obtendría?

05/05/2020

Con las nuevas fases de desescalada llegan nuevas incógnitas sobre **cómo se va a reanudar la actividad económica y social** y qué puede hacer la tecnología para ayudar en el proceso. En algunas informaciones se habla ya de la **toma de la temperatura** para entrar a ciertos comercios y locales e incluso de la **instalación de cámaras térmicas** que lo hagan de manera automatizada. Desde la perspectiva de la protección de datos, este asunto es algo delicado, sobre todo en el **ambiente laboral** y en las medidas tomadas para los empleados, y a nivel epidemiológico no es la práctica más avalada tampoco.

La Agencia Española de Protección de Datos (AEPD) habla de ese último punto para explicar los supuestos en los que se podría utilizar esta tecnología de una manera que no sea de lo más intrusiva: si hay que hacerse, que se haga, pero que al menos tenga el visto bueno de las autoridades sanitarias y que esté contemplado el **uso que se le va a dar a los datos de salud** que se recojan sobre esta práctica. Ya se ha denunciado esta práctica realizada por alguna empresa al considerar que vulnera derechos.

Las evidencias epidemiológicas sobre el control de la temperatura corporal como factor decisivo continúan siendo escasas

La Organización Mundial de la Salud (OMS) se pronunció sobre la eficacia de los escáneres térmicos para detectar a personas infectadas con COVID-19 y lo recogimos en este artículo. Dice que los escáneres térmicos son efectivos a la hora de detectar personas que han desarrollado fiebre como consecuencia del nuevo coronavirus, pero **no pueden detectar a las personas infectadas que aún no presentan fiebre** (algunas personas infectadas tardan entre 2 y 10 días en tener fiebre). Y no solo eso, sino que hay muchas personas que no llegan a tener fiebre pero sí desarrollan otros síntomas o que "la disimulan mediante el uso de antipiréticos".

Los métodos o aparatos **por los que se mide la temperatura** también son importantes, porque pueden dar resultados más o menos precisos sobre la temperatura, y tampoco hay, por el momento, ninguna directriz fijada sobre **qué temperatura deberían tomar** (hipotéticamente) los empresarios que introdujeran estas medidas y tecnologías.

“La fiebre, en sí misma, no es indicativa de COVID-19 ni de ninguna enfermedad concreta. Es **síntoma y signo de múltiples enfermedades**, no solo infecciosas”, aclaran desde el grupo de comunicación de la Sociedad Española de Microbiología a *Maldita Tecnología*.

Es necesaria esta especificación porque, como señalan, el principal problema epidemiológico “son los portadores presintomáticos y asintomáticos, que no tienen fiebre y escaparían a este control” y a cualquier otro basado en síntomas: “Un control de temperatura **no garantiza en ningún momento que no pasen personas contagiosas sin**

síntomas o con sintomatología leve. Por el contrario, es posible detectar como sospechosas a personas que no padecen COVID-19".

Sí que consideran que en un "escenario pandémico de vigilancia epidemiológica exhaustiva" tomar la temperatura puede ser "útil" como un "cribado sencillo para, de una forma muy inespecífica, detectar posibles casos activos de infección". La cuestión es que a nivel privado y de pequeños negocios **podría no ser "procedente"** debido a la "falta de competencia de los propietarios para interpretar este síntoma inespecífico", según señalan.

"El control de temperatura sin prescripción por parte de la autoridades sanitarias **no está recomendado** en ninguna de las circunstancias", resume Jesús Molina Cabrillana, secretario de la Sociedad Española de Medicina Preventiva Salud Pública e Higiene y jefe del servicio de Medicina Preventiva del Complejo Hospitalario Universitario Insular Materno Infantil de Las Palmas de Gran Canaria. "La fiebre puede tener **diversos orígenes** (no solo las infecciones), puede verse afectada por antitérmicos y no siempre está presente en COVID", explica.

Cuando comenzó la pandemia, este tipo de controles se implantaron en aeropuertos y puertos de algunos países, y ya entonces varios estudios determinaron que es un método con baja efectividad y un problema para el caso de los falsos negativos. Lo contamos aquí.

¿Mi temperatura corporal es un dato personal?

La temperatura corporal y un posible síntoma de fiebre o febrícula es un dato propio de salud que **no puede tratarse a la ligera**. En el Reglamento General de Protección de Datos (RGPD) este tipo de información goza de una protección especial.

"Este tratamiento de toma de temperatura supone una **injerencia particularmente intensa en los derechos de los afectados**. Por una parte, porque afecta a datos relativos a la salud de las personas, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, **se asume que una persona padece o no una concreta enfermedad**, como es en estos casos la infección por coronavirus", afirma la AEPD en un comunicado emitido el 30 de abril.

Aquí se añade la preocupación de que la temperatura corporal, aislada de otro tipo de información, no tiene por qué revelar la identidad de una persona, pero sí produce **cierto estigma al darse por hecho que con síntomas de fiebre esta padece COVID-19**: "las consecuencias de una posible denegación de acceso pueden tener un importante impacto", se explica.

La AEPD incide en que "estas medidas deben aplicarse sólo atendiendo a los criterios definidos por las autoridades sanitarias", tanto **en lo relativo a la "utilidad" que pueda tener como en su "proporcionalidad"**. Y que "esto es especialmente aplicable en los casos en que la toma de temperatura se realice utilizando dispositivos (como, por ejemplo, cámaras térmicas) que ofrezcan la posibilidad de **grabar y conservar los datos o tratar información adicional**, en particular, información biométrica."

Medidas aparte: ¿pueden las empresas hacer esto? "En España, las empresas tienen el deber de proteger la salud de sus trabajadores, velar por la salud de los empleados y sí

están legitimados para llevar a cabo determinados tratamientos, pero con algunas particularidades", explica Ruth Benito Díaz, abogada especializada en protección de datos y miembro de CovidWarriors, en esta videoconferencia (min. 33).

Y bajo ese supuesto, recogido en el art. 22.1 de la Ley de Prevención de Riesgos Laborales, es como la AEPD afirma que esta recogida de datos podría justificarse jurídicamente: porque **los empleadores tienen que garantizar la seguridad y la salud de las personas trabajadoras.** En principio, los datos de salud "los deben poder manejar únicamente personal sanitario, mutuas o los servicios de prevención de riesgos laborales, pero no la empresa en sí", añade Benito Díaz.

Jorge García Herrero, abogado especializado de Secuoya Group, sostiene que "cualquier control sobre el trabajador debe ser fundamentado documentalmente como **necesario, proporcional y limitado**" y que "cualquier medida de control de estas características realizada por la empresa a través de personal propio sobre toda la masa de trabajadores debería venir **precedida de una evaluación de impacto en privacidad**". Lo que viene a decir que si la medida es estrictamente necesaria, bien. Pero que si no, habría que plantearse una alternativa.

Sanidad no ha transmitido ninguna recomendación a los comercios de implantar estas medidas de control

A 5 de mayo, el Ministerio de Sanidad **no ha transmitido ninguna recomendación** a los locales y establecimientos que pueden ir abriendo en las distintas fases de desescalada **sobre la toma de temperatura corporal.** Si bien en lo que respecta a determinados comercios y servicios en una de las órdenes ministeriales del Boletín Oficial del Estado (BOE) se habla de establecer "el aforo máximo y las distancias mínimas que es necesario respetar", así como medidas para garantizar la seguridad, no hay nada especificado sobre impedir el acceso si alguien tiene fiebre. Desde el departamento también han confirmado a *Maldita Tecnología* que no hay ninguna recomendación al respecto.

En el artículo 3 de la Orden SND/388/2020 del 3 de mayo, además se especifica los casos en los que un trabajador **no podrá incorporarse a su puesto de trabajo** en un establecimiento comercial. Y en el caso del acceso de clientes que acudan a los establecimientos que abran, se fijan las siguientes pautas a cumplir:

> a) Se establecerá un sistema de cita previa que garantice la permanencia en el interior del establecimiento o local en un mismo momento de un único cliente por cada trabajador, sin que se puedan habilitar zonas de espera en el interior de los mismos.
> b) Se garantizará la atención individualizada al cliente con la debida separación física prevista en este capítulo o, en el caso de que esto no sea posible, mediante la instalación de mostradores o mamparas.
> c) Se establecerá un horario de atención preferente para mayores de 65 años, que deberá hacerse coincidir con las franjas horarias para la realización de paseos y actividad física de este colectivo.

¿Puedo negarme a que me tomen la temperatura si me lo piden en un establecimiento?

Es la gran pregunta, en vista de que muchos establecimientos pueden implantar este sistema si así lo consideran. En el caso de los trabajadores, se deben cumplir **una serie de requisitos para que la empresa pueda hacer un reconocimiento médico** que incluya la toma de temperatura en el marco de la pandemia de COVID-19: que la medida sea proporcional, idónea y necesaria y que cuente con el consentimiento de los trabajadores o de los representantes de los trabajadores, en su defecto.

Fabián Valero, abogado especialista en derecho laboral en el grupo Zeres, explica a *Maldita Tecnología* que hay dos derechos fundamentales que están en conflicto en este caso: **el derecho a la intimidad y el derecho a la vida e integridad física.** Ninguno desaparece al firmar un contrato con una empresa, pero sí que te integras en una estructura empresarial cuya dirección podrá organizar tu trabajo y determinar ciertas medidas.

Según el artículo 4 y 5 del Estatuto de los Trabajadores, los trabajadores tienen derecho a una **protección efectiva de la salud y una prevención de riesgos laborales adecuada**, pero también tienen la obligación de acatar instrucciones de la empresa. Frente a una pandemia que puede afectar al colectivo de los trabajadores, el reconocimiento médico se podría hacer solo con los **tres requisitos**, según Valero, entre ellos determinar si la medida es “idónea”, “proporcional” y “necesaria”. Si cumple con esos tres supuestos, podría hacerse si el trabajador lo consiente.

Y si no, con "una excepción, que dice que **una situación de riesgo inminente o grave para el resto de trabajadores**, para el propio trabajador o terceros, la empresa puede hacer un reconocimiento médico, con previo informe de los representantes de los trabajadores”, explica Valero.

Si soy un cliente, la situación puede ser complicada, sobre todo si es a través de una tecnología como una cámara térmica, **que probase que tengo una temperatura corporal elevada** y que luego se me identificase, en consecuencia. La AEPD no lo categoriza de ilegal siempre y cuando se haga una evaluación apropiada de la medida y se integre la protección adecuada al tratamiento de los datos personales obtenidos.

“En el caso de la comprobación de la temperatura corporal como medida preventiva de la expansión de la COVID – 19, esa base jurídica no podrá ser, con carácter general, **el consentimiento de los interesados**”, explica la AEPD. Con eso se refiere a que las personas afectadas que quieran entrar a un establecimiento **que impone esta norma** no podrían negarse a someterse al control de temperatura, por ejemplo, por lo que tampoco existiría la “libertad” de dar nuestro consentimiento para hacerlo. O lo tomas o lo dejas.

https://maldita.es/malditatecnologia/2020/05/05/camara-termica-control-fiebre-locales-comercios-coronavirus-datos/

¿Estoy obligado a dar mis datos en lugares de ocio por COVID-19? Puede ser legal siempre y cuando sólo los traten autoridades sanitarias y haya una norma para ello

29/07/2020

En comunidades como Madrid o Castilla-La Mancha se obligará a **los locales de ocio nocturno a registrar el nombre, número de teléfono y/o de DNI de los clientes** para poder contactarlos con rapidez en caso de que se registre un positivo en el establecimiento. En Madrid la normativa ya se ha aprobado, mientras que en Castilla- La Mancha sólo se ha anunciado.

Nos estáis preguntando **si las empresas privadas tienen potestad para recoger esos datos**. Abogados especializados coinciden en que no hay una respuesta de sí o no, pero que las empresas privadas no tienen legitimación para actuar escudándose en el "interés público". **Tendrían que ser las autoridades sanitarias quienes manejan los datos** y cuanto menos se den, mejor. Además, tiene que haber una habilitación normativa que permita a los locales hacer esa recogida. Os lo explicamos.

Pedir mínimo de datos al entrar a un local sí podría ser proporcional, pero con normativa acorde

Muchas personas se están preguntando si no se hace **un tratamiento de sus datos** personales al entrar en una discoteca de esta manera. La respuesta es afirmativa, al igual que se pueden tratar datos como el número de teléfono o el nombre para apuntarse en una lista de asistencia a uno de estos locales. Sin embargo, casi todo depende de **quién controla los datos que damos y para qué objetivo se usan**.

En este caso, se hace en el contexto de una pandemia donde se pueden aplicar ciertas concesiones en materia de protección de datos **si y sólo si quien maneja esos datos es una autoridad sanitaria**. Es decir, que podría estar justificado que recojan ciertos datos, como un número de teléfono o incluso tu identificación, pero **no para que los trate cualquier empresa privada** (en este caso los locales de ocio y las terrazas).

Además harían falta normas previas: "Esa medida necesitaría que **estuviera regulada en una norma para que fuera exigible**, y esto es así porque para poder recoger esos datos se necesita una **base de legitimación de las que contempla la ley,** y no encajaría en ninguna de las que tiene la normativa de protección de datos actualmente", explica **Verónica Alarcón**, abogada especializada en protección de datos en e-Privacidad.

La finalidad del uso de los datos tiene que estar definida

En el caso de apuntarte a las listas de un local, es la propia discoteca la que tramita tu asistencia usando los datos que tú has proporcionado. Con ello, te están diciendo cuál es la finalidad que van a cumplir: dejarte entrar a un precio u otro, por ejemplo.

En este caso, la finalidad es otra: ayudar a combatir una pandemia que afecta a nuestra salud, y ese papel **no puede desempeñarlo la empresa**, sino una autoridad sanitaria competente, como el Ministerio de Sanidad, escudándose en preservar el "interés público", una de las **bases legitimadoras** incluidas en el Reglamento General de Protección de Datos.

"Si lo que se pretende es que para entrar en un local sea obligatorio facilitar esos datos para usarlos para combatir la pandemia actual, hay que preguntarse **si eso es una medida proporcional o no**", explica Alarcón. Es decir: ¿va a ayudar realmente a gestionar la crisis sanitaria causada por COVID-19? Responder a esa pregunta es el primer paso.

¿Por qué no puede aplicar esta medida una discoteca y ya está? **Rahul Uttamchandani**, abogado especializado en tecnología y privacidad en Legal Army responde: "¿Para perpetuar la seguridad de tu negocio tienes que llevar a cabo ese tratamiento de datos? Probablemente no, sino que lo procedente es tomar las medidas de seguridad adecuadas, limitar el aforo, garantizar las medidas de higiene, etc.". El resto compete a Sanidad.

Si te obligan a dar los datos para entrar, no es un consentimiento libre

El Boletín Oficial de la Comunidad de Madrid ha publicado este 29 de julio que los establecimientos tendrán que llevar **un registro de fecha, hora y nombre y apellidos y número de teléfono** de las personas que pasan por él (un mínimo de datos) y que solo podrán almacenarlos durante **28 días**. La empresa no puede hacer nada con ellos más que derivarlos a Sanidad si son requeridos y deben avisarte que para eso los piden.

Ahora bien, en la resolución también dice que esos datos se recogerán gracias al "consentimiento del interesado", pero condicionan la entrada al local a ello.

Que una empresa que gestiona un local de ocio nocturno diga que se basa en el "consentimiento" de la persona para recabar esos datos (es decir, que trata mis datos porque yo se los estoy dando voluntariamente) **no sirve si no te van a dejar entrar si decides que no quieres darlos**.

Nos explicamos: si el consentimiento que damos a que se traten nuestros datos no es "libre", entonces no es válido. "En este caso lo que están haciendo **es someter el acceso al local a la condición de que se preste el consentimiento**. Eso invalida automáticamente el consentimiento: si yo no consiento, no entro", explica Uttamchandani.

"En un espacio privado los titulares se pueden reservar el derecho de admisión y pueden supeditar esa admisión al cumplimiento de los requisitos que quieran. Si quisieran funcionar solo con una app en la que todo el mundo tuviera que estar registrado para poder acceder, podrían pero **habría que justificar por qué esa app, por qué esa recopilación de datos, cuál es la finalidad pretendida, a quién se dan los datos**", continúa este abogado.

Con él coincide Alarcón: "La normativa de protección de datos obliga a **informar, en el momento de la recogida de los datos** (como por ejemplo en su política de privacidad) los destinatarios de la información, por lo que sí, es obligatorio que se especifique que se pasarán esos datos a Sanidad así como la finalidad de ese tratamiento".

https://maldita.es/malditatecnologia/2020/07/29/nombre-numero-ddiscoteca-covid-19-sanidad/

¿Podría en España decirte una app con precisión dónde hay una persona contagiada con COVID-19 o vigilar tu cuarentena? No si no está justificado el uso de esos datos

13/03/2020

China, Corea del Sur e Irán son los países que más sufrieron el contagio del COVID-19 cuando surgió el brote. En los tres se han elaborado **apps** que de una manera u otra se usan para **comprobar si una persona ha estado en contacto con otra con coronavirus.** En Irán incluso retiraron una que vigilaba las cuarentenas. Algunas más invasivas que otras pero con un punto en común: buscan que el Gobierno correspondiente pueda obtener información de las personas contagiadas. En España estas medidas de control del coronavirus **no son posibles**. Os explicamos por qué.

Necesidad de una fuente pública y oficial de datos personales

En China, en pleno pico de contagio del coronavirus, se puso en marcha una aplicación para que las personas pudieran **saber si cerca de ellas había alguien con COVID-19 y si corrían riesgo** de contraerlo ellas. Funcionaba registrándose con un número de teléfono y después introduciendo su nombre y número de identificación. La aplicación la sacaron en conjunto la Comisión Nacional de Salud, la Oficina General del Consejo de Estado y la Corporación de Tecnología Electrónica de China (CETC).

Los datos los obtuvieron además de la Comisión Nacional de Salud, del Ministerio de Transporte, el operador de ferrocarriles y la Administración de Aviación Civil de China. El sistema incluía personas que trabajaran juntas, fueran juntas a clase, vivieran en la misma casa, también al personal sanitario de los hospitales, a personas que viajaran en tren o avión, etc.

Una recogida masiva de datos, **entre ellos de los de salud y geolocalización**, que en España no sería tan fácil tratar. Menos sin consentimiento. El artículo 9 del Reglamento General de Protección de Datos es el que hace referencia al tratamiento de una categoría especial de datos personales, **entre ellos los datos de salud**. Estos están mucho más protegidos que el resto de datos personales y su tratamiento mucho más limitado (casi prohibido).

"En China está **conectada la historia clínica con el sistema de gestión de la polícia, del transporte e infraestructura**. Aquí no tiene cabida", asegura **Rahul Uttamchandani**, abogado especializado en protección de datos de Legal Army sobre el modelo de la app de rastreo de China.

El Gobierno no puede imponer que todos los ciudadanos se instalen una app concreta ni señalar sitios o a personas específicas

Esta es otra de las claves de cómo funcionan las aplicaciones dispuestas en China o en Irán. En este último país se sacó una al mercado que pretendía vigilar si la gente hacía

cuarentena o no con datos de geolocalización, registrando también el número de teléfono de las personas.

Jorge García Herrero, abogado especializado del grupo Secuoya, explica que no podría funcionar tampoco en España el que el Gobierno **obligase a toda la población a descargarse una app.** Y que aunque se pusiera a disposición una herramienta de rastreo, debería estar tremendamente justificada y **necesitaría el consentimiento de los usuarios.**

"Se podría hacer pero con un montón de limitaciones y de cuidados. Tampoco se podría hacer tan específica **para que no se lleve por delante intereses de otro tipo**", señala García Herrero. ¿Cómo cuáles? Bueno, imaginad que se señalara una cafetería concreta donde han pasado personas con coronavirus o un comercio. **¿En base a qué justificaría el Gobierno apuntar con el dedo de esa manera?**

Tengamos en cuenta que estamos hablando de una especie de mapa que pudieses consultar para ver por qué calles o sitios públicos ha pasado ua persona que ahora se habría confirmado que tiene COVID-19. Y que para ello se debe hacer **un tratamiento de los datos de salud (incluso por parte del Gobierno) que puede además terminar por estigmatizar** a parte de la población. Por eso son tan delicados los datos que entran en esa "categoría especial".

"No se puede amparar en la normativa el que el Gobierno **ponga esa información en el conocimiento de los ciudadanos**", dice Uttamchandani. "Una cosa es la información que tiene el Gobierno para gestionar los datos de la salud e infraestructuras, pero como ciudadanos no tenemos por qué saber esa información", recalca.

Que todo el mundo sea rastreado y geolocalizado sin estar contagiado no está justificado

Todos los profesionales consultados coinciden en que si se llegase a poner en marcha una herramienta de este tipo, debería hacerse de forma muy, muy justificada y que debería **atenderse el principio de minimización que recoge el RGPD**. Esto quiere decir que se debería aplicar a la zona más pequeña posible: "debería hacerse con **lo mínimo imprescindible** (área o número de personas involucradas en el seguimiento" y con la "obligación de restaurar la situación anterior en la forma más eficiente", explica **Ofelia Tejerina**, presidenta de la Asociación de Internautas.

Es decir, que costaría mucho que se hiciese un mapa de todo el país o de una comunidad completa porque las medidas tendrían **que asegurar que se usan solo los datos imprescindibles**. Así lo dice la ley europea:

Si en los países asiáticos han podido hacer algo así es porque los sistemas de vigilancia social que tienen activados (y tenían antes del coronavirus) no atienden a una **protección individual de la privacidad de la sociedad**.

"Tienen una regulación mucho más laxa, **su fortaleza es la materia de seguidad publica**. Tienen otro concepto de vulneración de privacidad y derecho de intimidad de la persona. EEUU, China... no tienen **nada que ver con el entorno europeo**", explica **Verónica**

Sevilla, abogada experta en protección de datos de ePrivacidad. Y que por eso dar acceso general a la ciudadanía de datos específicos de una sola persona (tanto su localización como sus datos de salud) **costaría mucho justificarlo.**

Ahora bien, ¿puede cambiar este escenario si la situación se agrava?

Debería agravarse mucho y aun así **no estaría del todo justificado que se pusieran datos ciudadanos al alcance de otras personas.** El reglamento europeo contempla algunas excepciones para tratar y usar información tan, tan sensible como es la de la salud. Una de ellas es "por razones de interés público en el ámbito de la salud pública, como la **protección frente a amenazas transfronterizas graves para la salud**".

Ajá. ¿Qué significa esto? Tiene relación con lo que os contábamos antes: si después de todo se decidiese que es necesario para el interés vital de la gente desarrollar una herramienta así, **las limitaciones serían muy duras.** Siempre acogiéndose al principio de minimización que decíamos arriba.

La cosa no queda ahí, porque además, para aplicar esa excepción concreta de la ley europea se necesita además **otra norma aprobada a nivel nacional o por los estados miembros** que apruebe que se puede hacer el tratamiento de datos, según nos explican Sevilla y Uttamchandani. Con sus especificidades, claro: qué se va a hacer, por qué se necesitan los datos, para qué se van a usar, qué derechos tienen las personas a acceder a ellos...

En definitiva, poner en marcha una app de rastreo como se ha hecho en países asiáticos no tendría cabida en España si pretendemos que los datos sean **precisos, fiables y procedentes de fuentes oficiales**. Si la situación de riesgo para la población aumentase, aun así costaría justificar que se pusieran a disposición ciudadana los datos de salud o de geolocalización.

¿Qué hay de la vigilancia de la cuarentena con una app?

"A día de hoy, dadas las cifras de contagio, el riesgo no es suficiente como para imponer medidas de vigilancia masiva como las de China", dice Tejerina. Las cosas podrían tomar otro cauce **si se declarara el estado de alarma**, que permite otro tipo de medidas como **imponer un toque de queda** o que haya **patrullas** vigilando que esto se cumpla.

Aun así, si esto pasara, el hecho de que el Gobierno pudiera **pedir los datos de salud a los centros sanitarios** y los de localización a las operadoras para usarlos en la gestión de la crisis del coronavirus **no implica que pudiera utilizarlo para vigilar las cuarentenas**. El uso de estos datos no sería proporcional para el objetivo a alcanzar: **que la gente se quede en casa**. ¿Qué quiere decir esto? Que probablemente haya otras medidas menos invasivas para controlar las cuarentenas **que no sea rastreando a toda la población** en tiempo real.

Un reciente informe de la Agencia Española de Protección de Datos sobre el coronavirus incide en ese punto: vale que el coronavirus es una emergencia sanitaria suficientemente grave como para que el Gobierno utilice los datos de salud de los hospitales sin pedir el consentimiento. Pero con fundamento y atendiendo al principio de minimización.

https://maldita.es/malditatecnologia/2020/03/13/app-coronavirus-espana-cerca-persona-contagiada-covid-19/

Cinco formas de hacer exámenes universitarios en tiempos de coronavirus: cuánto se vigila a los alumnos

12/05/2020

El sueño de todo estudiante es el anuncio inesperado de una suspensión general de exámenes. No tener que estudiar, no sufrir el estrés de las pruebas… Pero los sueños, sueños son. Las universidades han preparado o están preparando ya diferentes sistemas **con los que testar a los alumnos en sus exámenes finales** a distancia por la pandemia de coronavirus. Al ser educación superior no hay una norma común para todas ellas, sino que **cada centro puede elegir cómo realizarlos**. En algunos casos, son incluso los profesores de manera individual los que eligen en qué condiciones hacerlos.

Eso sí, en todas la tecnología forma parte del proceso en mayor o menor medida. En algunas ocasiones, se usa solo **para poder realizar el examen a distancia, y en otras para tener vigilado al alumno** y evitar las trampas. Aquí van cinco formas de las que las universidades están realizando exámenes, ordenadas **de menos a más control sobre la prueba y lo que hace el alumno**:

1. Sin ningún control sobre lo que el alumno hace o deja de hacer en casa y con su ordenador

Suena raro para un examen, pero hay universidades que por el momento **no han dispuesto un operativo especial** para poder hacerlos a distancia. Trabajan con las plataformas educativas que ya hay disponibles para **estar al día de las clases y hacer ejercicios**, como Moodle, pero sin poner especial énfasis en qué estará haciendo el alumno durante la prueba. En la Universidad Autónoma de Madrid, por ejemplo, funcionan así en muchas de sus facultades, como la de Derecho, según nos cuenta uno de sus profesores.

Las soluciones que han buscado en este caso es intentar **diseñar el examen de manera que no sea posible copiar**: por ejemplo, un comentario de texto que conlleve alguna reflexión. Aun así, según este profesor, es “imposible controlar que quien hace el examen es quien dice ser”.

2. Exámenes personalizados para evitar las trampas

Este es el sistema que están utilizando muchas facultades, **y para exámenes que se basan en números y problemas, más.** En la Universidad del País Vasco (UPV-EHY), uno de sus profesores, Julián Estévez, cuenta cómo ha elaborado exámenes prácticos para sus alumnos de Ingeniería Mecánica: los alumnos reciben un examen con **planteamientos diferentes (misma dificultad) en función de la letra que aparezca en su DNI**. Por lo que copiarse entre sí es un riesgo porque los números son diferentes.

También se usa Moodle para hacer el propio examen, que según cuenta Estévez tiene la opción de comprobar la dirección IP desde donde se hace el ejercicio, y Blackboard Collaborate para **hacer consultas y activar la cámara web**. “Tengo la preocupación de que cuando se hagan exámenes finales, cuando no haya confinamiento, vayan uno a casa

de otro a hacerlos", comenta Estévez, por ello la dirección IP también podría ser interesante de seguir en este caso. Por esto **ha puesto a prueba el sistema antes de llegar a los finales**: para testar que funciona y comprobar las calificaciones.

Este es uno de los casos por los que optan también en la Universitat de València, según explica a *Maldita Tecnología* Joaquín Aldas-Manzano, vicerrector de Estrategia, Calidad y Tecnologías de la Información de este centro: "Lo que hemos indicado para reducir este riesgo **es incrementar el peso de la evaluación continua** (de tal manera que el peso del examen final sea el menor posible) y realizar un **mix variado de tipos de prueba** (combinar test, con preguntas que exijan razonamiento, casos prácticos, proyectos…)", de modo que al final, de la manera que sea, copiar pueda salir mal.

3. Videoconferencias opcionales para hacer consultas, pero sin que sea obligatorio para identificar a los alumnos

Bueno, ¿pero si a veces se usan las videoconferencias para dar clases, también se usarán para los exámenes, no? No en todas, ya que **no se ha impuesto como un requisito para controlar una prueba**. Muchas universidades usan Blackboard Collaborate para hacerlas, pero en otras **se ha tirado de herramientas de vídeo como Meet (de Google) y Teams (de Microsoft)** por asegurarse de que no les va a dar problemas técnicos. Estas empresas están bastante integradas en los centros educativos de España, pese a ser de empresas privadas extranjeras.

En la Universidad Rey Juan Carlos (URJC) usan Microsoft Teams para complementar las pruebas con una videoconferencia **si el profesor lo requiere**. César Cáceres, director del Centro Innovación Digital de la URJC, explica que también se basan en Moodle para hacer los exámenes. Para identificar a los alumnos se guían por el registro de entrada que se hace en esa plataforma, pero **no hay una imposición de la universidad para comprobar quién está detrás de la cámara**: "Usando plataformas de videoconferencias los profesores pueden ver qué alumno hace el examen y pueden resolver dudas y preguntas", dice. Esto significa que para evitar las trampas tampoco hay nada específico dispuesto.

También en la Universitat Politècnica de Catalunya se ofrece **el uso voluntario de la cámara web para hacer los exámenes**, siempre y cuando no se grabe la sesión de la prueba. Recogen todos sus requisitos en este documento, donde rechazan herramientas de monitorización, ya que cuentan con plataforma propia para las clases: ATENEA.

4. Con reglas para la cámara web: activada en el caso de orales y mínimo el audio para los escritos

Hay otros casos en los que el uso de las videoconferencias es obligatoria. No hablamos de reconocimiento facial ni de identificación por medio de un programa, sino sencillamente de **mantener activada la webcam para que una persona pueda vigilar la prueba**. Tanto en la Universitat de Valencia como en la Universidad de Granada tienen normas fijadas. Si es examen oral, **se puede grabar para poder evaluarlo luego**. Si es escrito, tiene que funcionar Moodle para hacer el examen y **una plataforma de videoconferencia a la vez**, aunque la cámara no tenga que estar activada todo el rato. Sí que se usará al principio,

para que el alumno se identifique con su DNI y los profesores al cargo puedan comprobar que es esa persona la que se dispone a hacer la prueba.

Hablamos de cientos y cientos de alumnos conectados para hacer un examen a la vez, **con mínimo el audio activado para escuchar qué hacen**. Y que en un momento dado, si lo pide el profesor, **se pueda activar la cámara** para ver quién sigue detrás de la cámara.

5. Reconocimiento facial y monitorización del ordenador y el entorno para vigilar los exámenes

En otros casos se utilizan plataformas de las que ya hemos hablado, pero se les suma un componente más: un sistema que recoge **los datos biométricos de los alumnos antes de hacer el examen** y que además vigilan todo lo que hacen con su ordenador o en la estancia en la que están. El pack completo y, además, **automatizado**, conocido como proctoring. En la Universidad Isabel I, privada de Burgos, utilizan el sistema de proctoring de la empresa Smowl, un programa que ha sonado mucho **a medida que se ha ido acercando el período de exámenes** y que hace este tipo de vigilancia en tiempo real. ¿Cómo funciona?

Primero, con fotos del **alumno junto a su DNI**. “El alumno tiene que activar la cámara web para que se haga un registro constante de que el alumno es quien dice ser”, señala Ana Cristina García, directora de Innovación Educativa de la Universidad Isabel I. La imagen del alumno sumada a la de su DNI **es lo único que permite la validación de entrada al examen**. Una vez el sistema ha captado esas fotos, las guarda en una base de datos para ir comprobando a lo largo de la prueba que **la persona que está ante la cámara es la misma.**

“Otra herramienta es la monitorización del ordenador: mientras el alumno realiza el examen, tiene la cámara web activa para ver si abandona la mesa, por ejemplo. El sistema además detecta si usa otro tipo de programas, si tiene Skype abierto, si abren otra pestaña en el navegador…”, continúa García. En este caso, el examen se hace a través de Moodle y las consultas a través de Blackboard Collaborate, pero hay un añadido que controla todo lo demás: si el alumno se mueve por la sala, si hay otra persona al lado, si habla, etc.

¿Cuál de las medidas es más intrusiva con los datos de los alumnos?

La calidad de cada prueba la valoran en las propias universidades, ya que en muchas de ellas **cada profesor tiene “libertad de cátedra”** para realizarlo a su manera. La calidad de los métodos tecnológicos sí que se puede medir un poco más, sobre todo después de que algunos de los más intrusivos hayan generado alguna que otra protesta.

La Conferencia de Rectores de las Universidades Españolas (CRUE) emitió en un informe algunas medidas para ciertos tipos de pruebas que **en ningún caso contemplan el uso del reconocimiento facial,** por ejemplo, por considerarlo complejo en materia de legislación. También la Agencia Española de Protección de Datos (AEPD) se ha pronunciado, considerando que si se implantan estos sistemas, **se tiene que dar una alternativa al alumno** si quiere hacer la prueba en otras condiciones.

Jorge Campanillas, abogado especializado y delegado de protección de datos de una universidad española, explica en esta línea a *Maldita Tecnología* que “para grabar no necesitas el consentimiento de los alumnos” pero **sí para usar sus datos biométricos**, como imágenes de su cara. “El proctoring maneja datos sensibles, de alto nivel de protección, y afecta más a la privacidad”, asegura, por lo que la universidad tiene que poner los medios para que los sistemas **sean lo más seguros posibles.**

“El responsable del tratamiento de datos es la universidad y la elección del proveedor es importante”, añade, por lo que cualquier tipo de grabación o información personal del alumno usado durante el examen **debe guardarse de manera que no pueda difundirse**. Esto pasa por establecer acuerdos seguros con los proveedores de servicios (Google, Microsoft, Smowl, etc.) y que no se corra el riesgo de que se usen para otros fines.

https://maldita.es/malditatecnologia/2020/05/12/cinco-formas-examenes-universidad-coronavirus-vigila-alumnos/

Canarias, campo de pruebas de apps post-COVID: rastreo de contactos y pasaporte sanitario

23/05/2020

Se ha anunciado que las Islas Canarias serán el laboratorio de estudio de **dos soluciones tecnológicas de las que se ha hablado a nivel mundial** para afrontar el regreso a la normalidad en situación de pandemia. Una de ellas es una **aplicación para móviles de rastreo de contactos de personas** contagiadas de COVID-19, para enterarte de si has interactuado con alguien que tiene la enfermedad (te hablamos sobre ellas aquí). La otra es también una app, que almacenaría nuestro **historial clínico para "certificar" de alguna manera que ya hemos pasado la COVID-19** y así poder mostrarlo cuando viajamos a otros sitios: lo que se conoce como 'pasaporte sanitario'.

Esta última deriva de un proyecto que la Organización Mundial del Turismo (OMT) quiere probar a nivel mundial, según asegura el Gobierno de Canarias, y que en principio **se va a estrenar en julio**, con un vuelo al archipiélago. Esta aplicación tiene más sombras que luces, dado que el "pasaporte sanitario digital" del que tanto se habla para garantizar que una persona es "inmune" al coronavirus **no está avalado por la comunidad científica** ni tampoco hace mucha gracia en cuanto al uso y protección de los datos de salud. Te contamos lo que sabemos de ellas.

La aplicación de rastreo de contactos es un piloto descentralizado y no se sabe aún si se aplicará a toda España

Aunque el piloto se vaya a realizar en Canarias, esto **no significa que se vaya a crear sí o sí una aplicación para toda España**, simplemente que se va a probar su eficacia en el territorio canario.

La aplicación que se va a probar va a ser **descentralizada y funcionará por bluetooth**. ¿Qué significa esto? Principalmente, que los datos de contactos anónimos con otros dispositivos que recoja nuestro propio móvil a través de la aplicación **se quedarán en nuestro móvil**. Para saber más sobre cómo funcionan estas aplicaciones, te lo contamos en este artículo. La aplicación piloto se apoyará en una **tecnología llamada DP3T**, de la cual también te hablamos en ese artículo, y en un sistema que han elaborado Apple y Google (puedes leer sobre esto aquí).

Esto implica que la gente tendrá **un papel mucho más activo en todo esto y es esencial su participación** para que funcione: cuando a alguien le llegue un aviso al móvil de que ha estado en contacto con un COVID positivo esa persona tiene que, voluntariamente, ponerse en **cuarentena**. Además, el enfermo también tiene que colaborar: el médico le dará un código que **tendrá que introducir en la aplicación para que esta emita avisos al resto de móviles** con los que ha estado en contacto. La participación es clave y sin ella no funcionará nada del sistema, como contamos en este artículo.

La aplicación que llevará un “pasaporte sanitario digital” se probará en julio en un vuelo dirigido a Canarias, pero no es del Gobierno

La otra aplicación piloto se llama **Hi+Card** y su desarrollo lo anunció el Gobierno de Canarias el pasado 8 de mayo. Desde entonces, multitud de medios de comunicación se han hecho eco de ella para asegurar **que el primer “vuelo seguro” de COVID-19 va a llegar a Canarias con pasajeros no contagiados**. ¿Qué es lo que anuncian verdaderamente? “Esta aplicación se configura como un "pasaporte sanitario digital” para que “los pasajeros puedan viajar con tranquilidad y las compañías aéreas puedan, a su vez, aumentar la capacidad de sus vuelos”, explica la consejería canaria de Turismo, Industria y Comercio en un comunicado. Es decir, que en ella se podrá guardar **un certificado de nuestros datos sanitarios** que de alguna manera afirmen que estamos sanos y libres del coronavirus.

La idea del pasaporte sanitario no gusta ni a nivel científico, por la dificultad de asegurar la inmunidad, ni a nivel tecnológico, por el hecho de que **maneje información personal muy sensible, como los datos de salud**: la Agencia Española de Protección de Datos (AEPD) se pronunció contra estas aplicaciones. Meter en un mismo saco digital todo nuestro historial clínico es un proceso complicado.

Esta aplicación se quiere basar en la tecnología blockchain (de la cual te hablamos aquí), según sus desarrolladores: el Air Institute y Tourism Data Driven Solutions (TDDS). El uso de esta tecnología para **aplicaciones que gestionen datos sanitarios** está aún en pruebas y en este caso se contempla que se use a nivel internacional. Si llega a estar disponible para su descarga aquí, os podremos hablar de su funcionamiento.

“La aplicación permite registrar cualquier tipo de certificado y, en el contexto en el que estamos, de **certificado sanitario**. No utilizaremos otra información que la que certifiquen las autoridades sanitarias, por lo que no se da por hecho que una persona ya no se puede contagiar”, explican ahora a *Maldita Tecnología* desde Air Institute.

“No hay certezas con la COVID, no se sabe si vas a estar inmunizado”, explican a *Maldita Tecnología* desde la consejería de Turismo de Canarias. “Son gestos, fundamentalmente, lo que se persigue ahora mismo en Turismo, **recuperar la confianza**”, algo que pretenden conseguir en cierto modo con esta app. A su vez, aclaran que la idea es que se pueda mostrar un historial clínico **que diga que estás “inmunizado”** tras haber pasado la enfermedad para recuperar poco a poco el turismo.

El Ministerio de Sanidad es el que tendría que dar la orden a los sistemas sanitarios de las comunidades autónomas de que se **volcara la información sanitaria en la red que sustentaría esta aplicación,** para que al acceder nosotros pudiéramos mostrarla allá donde fuéramos y que se tuviera certeza de que es oficial.

Sin embargo, aunque el gobierno canario dice que el Ministerio está avisado, desde Sanidad explican que **no tienen información al respecto**. Air Institute nos dice que “todavía” no han contactado con el Ministerio porque están trabajando en la parte técnica, pero en TDDS dicen que no cuentan con él porque la aplicación “se basa en la inmunidad”, tal y como declaró su director a *National Geographic*.

Nos hemos puesto en contacto con la Organización Mundial del Turismo varias veces por correo, pero hasta el momento de esta publicación no han contestado la consulta.

A día de hoy no se sabe ni el grado de inmunidad ni la duración que genera haber pasado la COVID-19

Con el 'pasaporte sanitario digital' se busca justificar de alguna manera si tenemos COVID-19 o no y **si hemos pasado por la enfermedad.** Si se usara este supuesto para así "garantizar la seguridad" de un vuelo, por ejemplo, es algo con lo que la comunidad científica, por el momento, **no está de acuerdo.** La posición de la Organización Mundial de la Salud (OMS) es que todavía no se sabe cuál es el grado de "protección" que puede tener una persona tras haberse infectado con COVID-19 **ni tampoco cuánto dura**. Aquí explicaron los compañeros de *Maldita Ciencia* lo primero que estableció la organización sobre ellos.

La presidenta de la Sociedad Española de Inmunología (SEI), **África González**, coincide con ese factor: "Las personas que se han infectado y han desarrollado inmunidad estarán protegidas frente al virus. El tiempo de protección se desconoce, pero estaríamos hablando de al menos un año (en lo que se conoce con otros coronavirus convencionales) y de más de dos años en el caso de SARS y MERS. **No ha pasado suficiente tiempo para saber cuánto puede durar la inmunidad**, y si las personas han desarrollado memoria a largo plazo", nos explica.

En la SEI no consideran el pasaporte apropiado porque además de que no se sabe aún el tipo de inmunidad y la memoria generada frente al virus, **"el proceso de inmunidad puede cambiar en una persona"**, explica. Compara la reacción cruzada con otros coronavirus de infecciones comunes que pueden llegar a activar respuestas de reconocimiento del coronavirus actual (SARS-Cov-2).

Además de mencionar estos factores, las revistas científicas *Nature* y *The Lancet* han publicado contraindicaciones de los pasaportes que buscan garantizar que una persona está libre de COVID-19 **por considerar que esta medida podría causar discriminación socioeconómica** y también entre diferentes regiones y etnias. Los tests son necesarios para que esto funcione y el **acceso no está garantizado** a nivel global.

https://maldita.es/malditatecnologia/2020/05/23/canarias-pruebas-apps-covid-rastreo-contactos-pasaporte-sanitario/

Por qué la publicidad online sabe lo que te quieres comprar

24/02/2020

A Internet parece que nunca hay que contarle lo que queremos o nos hace falta. Los anuncios que vemos en las páginas web que visitamos lo confirman cuando nos muestran una y otra vez cosas que nos interesan, que habíamos visto antes o que incluso ya nos hemos comprado. El mecanismo que hace que esto sea así se denomina **“retargeting”** y es **una estrategia de márketing** basada en tu comportamiento online.

Un ejemplo práctico: supongamos que pasas un rato mirando vuelos para ir a Canarias aunque al final no lo compras. A partir de ahora, gracias al “retargeting”, **los anuncios de la compañía aérea te seguirán por toda la web**, probablemente mostrándote exactamente el mismo trayecto que tú querías hacer. Aparecerá cuando abras tu periódico favorito o al ver por Internet el partido de fútbol de la noche. ¿Qué pasaría si finalmente compras el vuelo? Pues que la aerolínea **puede vender esa información a empresas que recopilan este tipo de datos** para que estas, a su vez, se las vendan a otras compañías. Por ejemplo, a otras aerolíneas. En poco tiempo, estarías viendo ofertas a las Baleares por todo Internet.

Las cookies son una de las partes encargadas de recopilar los datos para el ‘retargeting’

Las cookies (de las que ya hablamos aquí) son las principales protagonistas en todo este proceso, porque son los principales rastreadores de la web junto a otras técnicas de perfilado como el **‘fingerprinting’**. ¿Alguna vez te has planteado cómo subsisten los buscadores de viajes como Skyscanner o Kayak? Por un lado, las compañías aéreas les pagan un porcentaje cuando el vuelo es reservado a través de su plataforma pero **su mayor fuente de ingresos viene de las galletitas informáticas**.

Cuando buscamos un vuelo en uno de esos buscadores, **descargan una cookie en nuestro ordenador** que almacena datos sobre nuestra búsqueda. Esa información luego se vende a compañías que se dedican a **crear ingentes bases de datos** que van recolectando sobre los usuarios, las llamadas data brokers, y estas le venden tus datos al mejor postor. En un caso así, probablemente a una gran aerolínea internacional que quiere saber qué tipo de vuelo te interesa para **mostrarte publicidad dirigida** directamente a ti y a tus intereses por todo Internet.

Pero si sólo me he metido en dos páginas, ¿por qué me encuentro los mismos anuncios por todas partes?

Aunque concebimos Internet como una serie de relaciones individuales en las que nosotros interactuamos con cada una de las webs de manera independiente, *la realidad es otra*. Como dice Eli Pariser, que es un activista político en Moveon.org y autor de "El filtro burbuja", **“entre bambalinas, la red está cada vez más integrada”**. Quiere decir que los sitios que visitamos y los servidores que guardan la información están **conectados entre sí.** ¡Por eso se llama red! Y por eso, las empresas se han dado cuenta de que **compartir tu información es lo que más rentable sale.**

Cuando interactúas con una página web con rastreadores activados como las cookies, estás **generando información que automáticamente se registra** y se envía a otros sitios online, sitios donde es más probable que te vuelvas a encontrar un anuncio similar. Incluso con las cookies desactivadas también puede sacarse esta información, como os contaremos próximamente.

¿Y quién coloca los anuncios?

Las redes publicitarias son empresas que se encargan de **llevar la información de un sitio a otro y fabricar el anuncio** en cuestión para cada uno de nosotros: es decir, que las zapatillas deportivas que estuviste a punto de comprarte no aparecen publicitadas mientras lees las noticias porque las ha colocado ahí el periódico, sino que hay una empresa detrás que está **en contacto con los anunciantes** que las colocan basándose en la información que ha llegado a través del rastreador.

“Los proveedores de publicidad comparten el identificador unívoco del cliente y de alguna manera el objeto de interés de la persona. **Lo que no comparten es la información específica sobre el cliente**. Es como si dijera que la cookie ‘5738392’ estuvo en Amazon viendo ‘este’ tema concreto”, explica a *Maldita.es* Javier González Recuenco, consultor de márketing digital y fundador de Singular Targeting.

Cuando arrancó la difusión de la publicidad online, los comerciantes y proveedores de anuncios web **pagaban por cada impresión que generaba un anuncio concreto** (cuánta gente lo veía o cuánta gente hacía clic en él). Hoy en día, el pago se basa en cómo actúan los usuarios después de haber visto o interactuado con un anuncio: ¿terminan comprando el producto? ¿Miran otro parecido? Este tipo de comportamientos **es lo que hacen que un anuncio valga más o menos**. Como operan en entornos digitales, lo que venden es la ‘influencia’ que logran ejercer en los usuarios, normalmente ofreciendo huecos para publicidad o directamente vendiendo los datos.

Eso no quita que cada página tenga contratos directos con anunciantes como la **publicidad tradicional**: desde bancos a oenegés, tiendas de muebles, de ropa deportiva, consultoras, eventos próximos, fundaciones, etc. Igual tú no estás pensando en comprarte un coche porque ni siquiera tienes carnet de conducir, pero cuando entras en tu periódico todo lo que ves es el último modelo de la marca X: esta es publicidad tradicional como la que veías en el periódico de papel y que **nace de acuerdos entre el anunciante y el medio o la web** que estés consumiendo.

Vale, si ya me he comprado unas zapatillas de deporte, ¿por qué me siguen bombardeando con más zapatillas?

Es muy improbable que dos días después de que te compres online unas zapatillas para hacer running, decidas comprarte otro par. Lo que sí es probable es que sigan apareciendo por todos los recónditos espacios de Internet junto a otros zapatos y unos maravillosos calcetines antisudor a juego. ¿Para qué? ¿No detecta el algoritmo que ya tengo unas?

Pariser explica que las empresas que utilizan la técnica del “retargeting” a gran escala, como puede ser Amazon, lo hacen para **no tener que “aceptar un ‘no’ por respuesta”**. Es

decir: si crees que no quieres algo, yo voy a hacer que sí lo quieras. Y si te has comprado unas zapatillas deportivas, **eres susceptible de comprar productos relacionados** con ellas.

Concretamente, Amazon incluso organiza sus gigantescos almacenes en base a un concepto casi inventado**: almacena juntos cantidad de productos que no tienen por qué estar relacionados entre sí**, porque ha extraído de los patrones de compras de los usuarios que después de unos cuantos clicks por la web, puede que llegues a comprarlos juntos. Y así, los trabajadores los encuentran todos en un mismo lugar.

Por ejemplo, si te compras un móvil nuevo, es probable que en unos días sientas la necesidad de ponerle una carcasa o comprarte unos cascos. Esto Amazon lo sabe porque **nos pasa a todos los seres humanos** y ya tiene pensada su manera de organizar sus almacenes y de ponerte a ti la publicidad en base a ello.

González Recuenco argumenta que la industria publicitaria aplica esta técnica sobre todo su público potencial -que abarca todo Internet- a la espera de **al menos influir en un segmento pequeño de personas.** Concretamente, en “molestar mucho al público en su totalidad” a cambio de que algún porcentaje pique y compre. Y que eso ya es suficiente logro.

Que dejen de perseguirte por la web no es algo que esté al alcance de nosotros los morales: **la huella digital no se puede borrar**. El márketing digital tiene muchas artimañas para averiguar cosas de nosotros y es muy difícil ponerles freno con tareas sencillas. Aun así, **puedes empezar por limitar las cookies** que dejas que pongan las páginas web en tu ordenador. Te contamos cómo rechazarlas en este artículo.

https://maldita.es/malditatecnologia/2020/10/11/por-que-la-publicidad-online-sabe-lo-que-te-quieres-comprar/

¿Qué son las cookies?: por dónde viajan y cómo limitarlas

24/02/2020

No son las que se comen, y decididamente son menos apetecibles de tener guardadas en el armario que representa nuestro ordenador o móvil. Las cookies informáticas son **pequeños archivos que las páginas web descargan en nuestro ordenador o móvil** cuando accedemos a ellas y que permiten a los servidores **rastrear nuestra actividad** mientras navegamos en Internet, recordar nuestras preferencias y mantener sesiones activas al registrar los nombres de usuario y contraseñas que utilizamos.

Conocerlas las conoces, porque a día de hoy es imposible entrar en una página web sin que te introduzcan su política de cookies en cuadros que en ocasiones **tapan mitad de pantalla** y no desaparecen hasta que las **aceptamos o rechazamos** (si es que da la opción). Ahora bien, quizás no sepas lo que hacen y aceptarlas sin saber qué se está autorizando igual **no es la mejor idea**, sobre todo teniendo en cuenta que por lo que siempre optamos es por deshacernos del incordio que no nos deja seguir navegando: aceptamos todo y como si nada.

Os contamos cómo funcionan estos ficheros y **por qué hay que aceptar su uso cada vez** que accedemos a una página web.

¿Cómo llegan las cookies a tus dispositivos? Pensemos en una cafetería y un camarero con ceguera

Para explicar cómo llegan los pequeños archivos de texto que son las cookies a nuestro ordenador vamos a **sustituir a los dominios** (las páginas web), por **cafeterías** y al **servidor**, que es la máquina que se encarga de poner a disposición los datos de esa página y a quien pides lo que necesitas (acceder a una página web), por **un camarero**. El camarero es el que va a escuchar tu comanda y te va a dar lo que pides. Con un condicionante: **tiene ceguera.**

El camarero **no es capaz de reconocernos como cliente** de ninguna manera si nunca hemos interactuado con él, así que para poder reconocernos y ser atendidos en la cafetería en cuestión, nos dará una **entrada que nos identifica**: una cookie. Además esta es una cafetería un poco pija así que sólo puedes entrar si tienes este ticket con forma de galleta que es personal e intransferible.

Por tanto, las cookies son identificadores que **no puedes ponerte tú mismo** como usuario pero que son necesarias para acceder a una página web.

Seguimos con nuestra metáfora: el papel de entrada con tus datos que te ha dado el camarero está encriptado, es decir, que **solo él lo puede descifrar**. Por eso **utilizar el de otra cafetería sería inútil**. Si otro día vuelves a la cafetería, podrás darle la misma entrada, donde él ha apuntado tu comanda y el camarero **se acordará de ti y de lo que pediste**: un café con leche y una napolitana. Que traducido viene a ser la **interacción** que tuviste en una página web: qué secciones visitaste, dónde te detuviste más tiempo, si marcaste alguna publicación con un “Me gusta”, si pinchaste en algún anuncio...

Como la entrada te la ha dado la propia cafetería para acceder a ella, hablamos de una o varias cookies instaladas por la propia página web. A esas las llamamos **cookies funcionales** porque **permiten que la página web funcione y pueda identificarte** cuando accedes a ella y saber desde donde te conectas, a través de por ejemplo, una dirección IP. Así, esa página anfitriona puede recordar lo que hacías en ella.

Cookies de terceros: vienen de otros servidores y sirven principalmente para colocar la publicidad adecuada y analizar el comportamiento

Ponle que llegas de nuevo a la misma cafetería y el camarero te da una nueva entrada. Pero no solo te da esa, sino que **te da otra entrada más** que incluye una identificación distinta, a pesar de que no sea de su cafetería, sino de **otra que le ha dado permiso** para darte ese papel. Cuando decides irte de esa cafetería a una distinta, el nuevo camarero te pedirá las entradas que tengas. Ambos mozos están en contacto entre sí, y además tiene tu papel de identificación, así que **ya cuenta con información sobre ti.** Y también sabe que vienes de una cafetería distinta.

Esta trazabilidad es la que describe las **cookies de terceros**: son ficheros colocados por otros servidores y páginas distintas a la que estás visitando y sirven para que esas páginas externas **puedan saber tus preferencias** cuando navegas. Con eso, principalmente, logran personalizar la publicidad para que se ajuste más a tus gustos, hacer análisis de impacto sobre las publicaciones más visitadas, saber qué colocar primero para que te llame más la atención… Es decir, forman **pequeñas fichas que analizan el comportamiento** para que las empresas tomen ese tipo de decisiones.

Son estas cookies las que, por ejemplo, permiten que la web de tu periódico de cabecera sepa que estás interesado en comprar una tostadora que has estado mirando en otra web y por eso te llena cada espacio publicitario de los diferentes modelos que más te han interesado.

¿Por qué es obligatorio aceptar alguna de ellas, entonces? ¿Qué pasa si no lo haces?

Más que a galletas, las cookies se parecen a las lentejas y al refrán que toda madre ha tuneado alguna vez para torturarnos: si las quieres, te las comes, y si no… también. Las que crean polémica por los **perfiles personalizados** y de consumo que se hacen de los usuarios son las de terceros, porque al final se trata de que **una página web que no estás visitando obtiene información** de ti, llegues a hacerlo o no.

En Europa, los proveedores de servidores web están obligados a avisarte de que están usando cookies que contienen información sobre ti y darte la opción de elegir si aceptas el rastreo o no. Esto es gracias a diferentes directivas europeas: la ePrivacy relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento General de Protección de Datos (RGPD), la máxima norma europea que concierne a los datos personales*. Sin embargo, no todos los sitios web te dan la opción y hay otros que lo hacen a través de un laberinto de accesos. O, directamente, con anuncios incomprensibles como muestra este abogado:

Hay un tipo de cookies (normalmente llamadas **obligatorias** o **funcionales**) que son las únicas que no pueden rechazarse, ya que procuran el buen funcionamiento de la página web anfitriona. Otras, como las de “estadística”, “personalización de contenido”, “publicidad”, “análisis de navegación”, “almacenamiento” o “medición”, sí son prescindibles.

¿Qué estás rechazando cuando no autorizas este tipo de cookies? Pues, por ejemplo, que cuando vayas a una nueva web/cafetería, el camarero de la anterior no le pueda contar al nuevo barman qué cosas te gustan o cuál es ese producto capricho que estuviste mirando en la web anterior pero que finalmente decidiste no comprar. **¿Qué hace el camarero con esta información?** Posiblemente ponerte ese oscuro objeto de deseo por toda la web a ver si así consigue que lo compres.

¿Cómo las rechazamos? ¿Se puede hacer siempre?

Según la “Guía sobre el uso de las Cookies” de la Agencia Española de Protección de Datos (AEPD), **no interactuar con el cuadro de aviso del que hablábamos antes y seguir navegando** en la página web también implica que aceptamos la configuración de las cookies **venga como venga** (que en algunos sitios suele ser con el pack completo activado). Y el problema es que en muchos sitios esto es así, por ejemplo y sin ir más lejos, en Twitter.

Algunas páginas web te darán la opción de **"Rechazar todo"** pero otras no, sino que te expondrán su Política de Cookies sin botones extra. El primer paso para rechazarlas será siempre **"Cambiar la configuración"** o pedir más **"Información y ajustes"** haciendo clic en estas frases o en las variantes que aparecerán (más pequeño y más escondido) junto a la opción de "Aceptar". Hay varias modalidades de estilo para rechazarlas, pero una vez que conozcas dos o tres, te sonarán todas. Te dejamos algunos ejemplos:

Como no todas las página te darán una opción tan directa, lo que también puedes hacer es "desconectar" las cookies desde el propio navegador. Todos ellos dan instrucciones bastante claras de cómo hacerlo, así aquí te dejamos un enlace directo para que eches un vistazo: para Google Chrome, para Mozilla Firefox, para Microsoft Edge y para Safari.

https://maldita.es/malditatecnologia/2020/02/24/cookies-que-son-por-donde-viajan-y-como-limitarlas/

'Fingerprinting' o cómo se crea tu huella digital

20/03/2020

Nos habéis preguntado por un concepto que habréis leído en muchos sitios y que tiene que ver con **prácticamente todo lo que hacemos en Internet**. La huella digital está formada por todos los **datos que vas dejando en la red,** tanto si es a propósito como si no. Hay muchas actividades que hacemos de manera consciente en el mundo online, como subir cosas a redes sociales, compartir contenido, ver series y buscar información sin parar. Todas esas acciones dejan rastro en Internet y ayudan a crear **una especie de identidad basada en datos sobre tu persona** y lo que sueles hacer cuando te conectas.

¿Qué pasa con el rastro que dejamos de manera inconsciente? Principalmente, lo recogen diferentes rastreadores como las cookies, de las cuales os hablamos aquí. En muchos casos, las cookies se pueden desactivar, pero existen otras técnicas para recopilar información de manera exhaustiva y que pueden **funcionar sin que demos nuestro consentimiento**. Una de ellas es el llamado **"fingerprinting"**, que es un verbo en inglés formado a partir de "fingerprint": huella dactilar.

Todas las maneras por las cuales se pueden recoger datos sobre ti

"Fingerprinting" es como se llama a la recolección de información que termina conformando tu huella en la red. Es una técnica que recoge datos de los propios dispositivos, datos que no tienen tanto que ver con lo que miras online, sino cómo lo haces: **sirve para identificar al dueño que maneja el móvil u ordenador** y crear un perfil en torno a él.

La **Agencia Española de Protección de Datos (AEPD)** señala que esta práctica es efectiva porque "dado que lo habitual es que las personas no compartan sus equipos, ya sea este un teléfono móvil, portátil u ordenador de trabajo, **individualizar el terminal supone individualizar a la persona que lo utiliza**". Es decir, que los dispositivos que usas sirven para ficharte.

¿Y qué se puede recoger? Si decimos que de todo… ¿crees que estamos exagerando? A pesar de sonar generalista, es así: la cantidad de datos que se pueden extraer de un aparato cotidiano como un móvil u ordenador **son cosas que nunca pensarías**. La cuestión es que son datos **más técnicos** del propio aparato y que puede que pienses que no son útiles para saber cosas de ti.

¿Por ejemplo? El **idioma** en el que lo manejas, la versión y la configuración de tu **navegador**, las **aplicaciones** que tienes instaladas, la **zona horaria** en la que te encuentras, el **nivel de batería** que tiene el terminal y cuándo la personita lo usa más, **acelerómetros** (una herramienta que mide la velocidad a la que se mueve el dispositivo), la **memoria** que has usado, si usas programas para **bloquear la publicidad**, y un largo etcétera.

Quizás recuerdes aquella vez que se viralizó en Twitter que la empresa de coches con conductor Uber subía los precios si detectaba que te estabas quedando sin batería. Uber aseguró que no lo hacían, a pesar de que sí que admitieron que **podían acceder al nivel**

de batería del teléfono en cuestión. Es decir, que Uber ya tiene ese dato sobre tu móvil que puede unir a muchos más y, al mismo tiempo, a la cuenta que tienes con ellos.

La legalidad de esta recogida depende de los fines para los que se usen los datos

“Contrariamente a lo que pueda pensar, el perfilado no se limita a recopilar y analizar los hábitos de navegación del usuario o las búsquedas que realiza en servidores. Las técnicas más avanzadas permiten **registrar los movimientos que realiza el usuario a través de la página web con el ratón**, examinando en qué partes de la pantalla se detiene por más tiempo”, explica un informe sobre la huella digital de la AEPD, que es el organismo del Gobierno que se encarga de hacer cumplir la Ley de Protección de Datos.

Todo esto se realiza sin el consentimiento del usuario, por eso no está muy claro si es legal o no, ya que depende de para qué se usen esos datos. Por ejemplo, la AEPD dice que es legal si se utiliza para lo que se llama “mecanismos de autenticación de factor múltiple”, es decir, para identificar de más de una manera que **la persona que está detrás del dispositivo eres tú** y no alguien que quiere suplantar tu identidad. Sin embargo, también pueden usarse para “hacer un seguimiento de los usuarios durante su navegación web y recopilar información sobre sus hábitos e intereses sin que propio usuario sea consciente de ello”.

La AEPD considera que esta técnica y la entrega de los datos que se pueden sacar con ella debería hacerse **sólo si las personas dieran su consentimiento para ello** porque la “finalidad para la que se recaban los datos” es bastante delicada. Al fin y al cabo, se está creando un **perfil** de una persona analizando su actividad online para luego utilizar con otros fines. ¿El principal? La publicidad dirigida: los negocios quieren saber qué tipo de consumidor eres.

Además, en esa larga lista de información que sacan de tus dispositivos y lo que haces con ellos se puede encontrar información relacionada con la orientación sexual de la persona, su religión o su lugar de procedencia: datos tan, tan sensibles que son clasificados en una **categoría especial** según el Reglamento General de Protección de Datos europeo. A esa categoría especial se le inyecta un refuerzo de protección, de ahí que la AEPD ponga incluso más en duda la legalidad del “fingerprinting”.

Si no te sientes muy agusto con la idea de que estén recopilando datos sobre lo que te gusta y te deja de gustar con fines principalmente publicitarios y comerciales, puedes visitar nuestro repositorio de alternativas digitales, aún así, tenemos que recordar que a estas alturas, la huella digital es **prácticamente imposible de borrar del todo** de Internet, lo que no quita que podamos mejorar su higiene de ahora en adelante. ¡Esperamos que te sirvan!

https://maldita.es/malditatecnologia/2020/03/20/fingerprinting-o-como-se-crea-tu-huella-digital/

Mi robot de cocina me pide que acepte una Política de Privacidad y mi tele una de cookies

09/03/2020

Las televisiones de tubo, esas que tiene culo y necesitan muchísimo espacio, están por extinguirse. Si todavía tienes una, a la hora de cambiarla es más que probable que en la tienda quieran convencerte para que te compres **una novísima Smart TV** porque se puede controlar por la voz, recuerda tus programas favoritos, te hace recomendaciones personalizadas, puedes jugar en ella online, instalar apps… Suena todo genial, hasta que llegas a casa y **al configurarla te pide aceptar una extensísima política de privacidad y otra de cookies**. ¿Y esto?

Sencillamente **es porque está conectada a Internet** e igual que aceptamos ciertos requisitos cuando navegamos por una página web, una televisión inteligente también está **obligada a avisarte** de que lo que veas (y a veces lo que que digas cerca de ella) se puede grabar y almacenar.

Y no sólo la tele: lavadoras, impresoras, webcams, frigoríficos, equipos de música, coches… Se conectan a la red y entre sí, por lo que adquieren **nuevos usos que no habíamos experimentado antes y que, por tanto, no sabemos controlar al principio**. La idea del *hogar inteligente* se vende con promesas de comodidad, eficiencia y experiencias nuevas y son numerosas estimaciones las que sitúan **entre 20.000 y 50.000 millones los dispositivos** conectados a una red de aquí al **año 2025**.

Las mil y una páginas de condiciones para usar mi robot de cocina

Resulta que el robot de cocina no es solo robot porque pica y guisa sin ayuda o porque guarda las recetas que yo quiera, sino porque **se conecta a la misma red que se conecta el ordenador y transfiere datos**.

Muchos de esos requisitos son necesarios para que el sistema del robot funcione y que los fabricantes **obtengan información para mejorar el dispositivo o arreglarlo** en caso de que sufra un fallo generalizado. Ahora bien, hay otras para las que no. Como en el caso de la tele (que guarda cuánto tiempo la tenemos encendida, si cambiamos de canal cuando hay anuncios, si tenemos Netflix, etc.), la Monsieur quiere saber cuánto tiempo la utilizamos, en qué función, qué ingredientes ponemos, a qué hora la enchufamos… **Información que luego puede anonimizarse y venderse a terceros**, como reflejan algunos estudios.

"Hay que ser conscientes pero que la privacidad viene a un coste, las otras potencias mundiales están avanzando en inteligencia artificial mucho más cuando son capaces de acceder a datos masivos de usuarios, **eso inevitablemente redundará en ventajas estratégicas de todo tipo**", explica a *Maldita Tecnología* Sergi Udina, que es un maldito que nos ha prestado sus superpoderes y es doctor en microelectrónica y profesor de Machine Learning en la Universidad de Barcelona.

Mi aspiradora inteligente puede hacerse con un plano de mi casa y eso debe importarme

Todo lo que recoge en casa un aparato inteligente se guarda en la nube (que definimos aquí). **Pero no se queda ahí para los restos sin que nadie la use.** Las aspiradoras inteligentes, por ejemplo, saben moverse por una casa porque tienen sensores que van registrando cómo esquivar el sofá o la mesa del comedor. Para ello, guarda un plano en su sistema de lo que va recolectando.

Imagina que ese plano se vendiese a otra empresa. Quizás no vaya acompañado de tu nombre, edad y tu dirección exacta (porque los datos se suelen anonimizar cuando se ceden a terceros), pero a una empresa de muebles sí que le puede interesar que **en un barrio concreto las casas son de determinada manera** y que **el rango de edad de la gente que vive allí** es de 24 a 30 años. Así pueden dirigir su publicidad de forma segmentada y masiva y decidir si abre una tienda en la zona, qué tamaño de sofás debería vender en ella y **qué precios decide poner**. Las empresas toman esta clase decisiones en base a datos agrupados que nosotros, los ciudadanos, a veces damos sin saberlo.

"Puede parecer difícil imaginar por qué información básica como qué comemos o cuándo encendemos las luces es tan valiosa, pero es el tipo de información que cuenta cuándo estás en casa y quién eres", dicen los autores de un estudio sobre el hogar inteligente de la Fundación Mozilla.

El hackeo en marcha: ¿se puede pasar a controlar una webcam?

“La gente tiene que ser consciente de que cualquier dispositivo doméstico conectado la red es **susceptible de tener un problema de seguridad** y de suponer un riesgo para la privacidad”, asegura Marta Beltrán, investigadora y directora del Grado de Ciberseguridad de la Universidad Rey Juan Carlos.

Beltrán defiende que la seguridad de los aparatos inteligentes que utilizamos en casa **flaquea porque no suelen estar tan bien protegidos como otros dispositivos**. “Cuando se descubre una vulnerabilidad en un sistema operativo de un móvil o un ordenador, se pone un parche. Si se descubre en una nevera, se queda sin parchear”, porque **los diseñadores no son empresas tecnológicas acostumbradas a lidiar con esas inseguridades**, sino fabricantes de electrodomésticos.

Nos explica un método por el cual se puede controlar la red a la que están controlados muchos dispositivos llamado “denegación de servicio”: consiste en **controlar una red enorme de miles de dispositivos que ya están infectados** con un malware. En un momento determinado, la persona que los controla los fuerza a comunicarse todos a la vez con la red que quieren hackear. Esa red recibe miles de millones de mensajes a la vez, no es capaz de gestionarlos y se cae. En ese momento es más vulnerable.

¿Qué ha pasado en los últimos años? Que las redes de aparatos infectados se hacen cada vez más grandes porque **los dispositivos domésticos son más “tontos”** que un ordenador o un móvil más sofisticado y son un blanco fácil, nos cuenta la académica.

Los casos que hemos mencionado son reales y una brecha nos podría tocar a nosotros si empezaramos a estirar las capacidades de la domótica: una red WiFi personal comprometida a través de una simple bombilla, espionaje a integrantes de la casa por una webcam o asistentes de voz hackeados con un láser.

Al hogar inteligente le queda todavía tiempo para instalarse ampliamente en España

En España, un informe sobre el Internet of Things (IoT) conducido por Telefónica expone que “los consumidores de IoT residencial comienzan buscando ‘control de gastos’ y optimización del consumo energético”. En ese marco, **los dispositivos más usados son las Smart TV**, seguidos de los usados para controlar la electricidad. “Aunque el interés a medio plazo es creciente y constante, **es prematuro todavía poder hablar de hogar conectado** de un modo genérico”, continúa el estudio.

En otro informe de 2017 la Fundación Cotec dice que pese a que España se considera un país “líder” en la propuesta de iniciativas que tienen que ver con el IoT, **en capacidades para aplicarla es un “seguidor”**. Es decir, que no ha avanzado demasiado en su aplicación.

"Sobre todo es en Japón donde desde siempre han apostado fuerte por estas tecnologías, pero en general la Asia más desarrollada y con especial potencia China, **ya que la (práctica ausencia de) ley de protección de datos permite que la apuesta estratégica** por el IoT avance enormemente sus capacidades de desarrollo", asegura Udina.

Por el momento, **no hay organismos públicos** como el Instituto Nacional de Estadística que estén **recopilando información sobre el uso de dispositivos inteligentes** en los hogares españoles, más allá de la conectividad a Internet o los aparatos electrónicos que se usen en ellos.

Con estas expectativas, lo que nos queda es por decir que hay que ser prudentes con la manera en la que introducimos dispositivos conectados en casa. Cierto es que pueden traer comodidad a algunas tareas domésticas, pero es importante ser conscientes de lo que conlleva. Nos podemos ahorrar pequeños disgustos con gestos como cambiar la contraseña de acceso al dispositivo cuando lo compramos. Y, sobre todo, leyendo los términos y condiciones de lo que estamos poniendo a funcionar.

https://maldita.es/malditatecnologia/2020/03/09/robot-de-cocina-privacidad-television-cookies-hogar-inteligente/

Asistentes de voz: qué datos guardan de mí y cada cuánto los borran

18/08/2020

Seguramente, hayas oído hablar mucho de Alexa, de Google Assistant, de Siri y de lo intrusivos que son los **asistentes de voz insertados en los altavoces inteligentes** que tenemos en casa o en el móvil. Que si nos escuchan, que nos espían…

Es cierto que se han enfrentado a más de un problema de privacidad desde que se comercializaron en 2018 para los hogares, especialmente cuando se supo que tenían a personas humanas escuchando algunas de nuestras conversaciones, supuestamente para "mejorar" el servicio, y que se ha demostrado que se activan cuando no deberían y grababan conversaciones privadas. Aquí buscamos explicarte cómo funcionan, qué datos guardan y durante cuánto tiempo lo hacen.

"Alexa, proponme un regalo para San Valentín"

Se llaman altavoces inteligentes porque contienen un programa automatizado que **se activa con una palabra clave** como "Alexa" (para el altavoz Echo de Amazon)", "Ok, Google" (el asistente de Google) u "Oye, Siri", el conocido asistente de los iPhone de Apple. Justo después se hace la petición, **que es lo que el asistente va a registrar y guardar**.

Son sistemas basados en el **aprendizaje automático**, un concepto que te explicamos más a fondo en nuestro glosario. Esto quiere decir que **va introduciendo nuevos temas constantemente**, en función de lo que va escuchando y lo que le piden hacer.

¿De dónde salen los resultados que cantan los asistentes con su tono robotizado? Amazon Devices explica a *Maldita.es* que Alexa obtiene su información de una **"variedad de fuentes confiables"** y que depende de si la petición puede estar relacionada con ***skills* de terceros** (herramientas creadas de otros servicios que no son Amazon). Si le pides que reserve un Uber por ti, usa información extra incluida en el sistema, al igual que cuando le das la orden "léeme las noticias de El País de hoy".

Las fuentes a las que hace referencia Amazon Devices van desde la RAE hasta Wikipedia; si pides que te recomiende una película puede acudir a IMDb y si quieres reservar en un restaurante a Yelp. Cuando no tiene donde acudir porque la petición no tiene una respuesta clara (si por ejemplo le pides que te proponga un regalo para San Valentín), tirará de la **configuración de frases que tiene establecida**.

El Asistente de Google, por otra parte, utiliza el motor de búsqueda de Google para ofrecer respuestas. Lo mismo que **si abrieras tu navegador y lo escribieras en la barra de búsqueda**. Piensa en cuando buscas el tiempo de Madrid en Google: no solo te ofrece enlaces a portales meteorológicos, sino que además te muestra un gráfico con temperaturas y días. El Asistente funciona como **ese apartado extra de información**: interpreta resultados y los verbaliza sin tener que llevarte a otros servicios o webs.

Al final, estos asistentes funcionan como una vertebra más del resto de acciones que hacemos en Internet: buscar cosas, comprar, leer, usar redes sociales, trabajar… No solo son las grabaciones de nuestra voz lo que almacenan, sino **el contenido que consumimos a través de ellos** y que deja una huella digital.

¿Durante cuánto tiempo se quedan con las preguntas y los comandos?

Esta es la pregunta que todas las tecnológicas prefieren esquivar, ya que la mayoría de ellas configuran los asistentes de modo que **las grabaciones se queden almacenadas hasta que el propio usuario decide eliminarlas.** Lo que les preguntamos se guarda en la nube y puede ser usado posteriormente por las empresas para mejorar los asistentes (según consta en sus políticas de privacidad).

"El historial del Asistente es parte de tu actividad en la web y la app, así que **el período de tiempo que escojas ahí también incluye al historial del Asistente**. Por lo demás, las interacciones de los usuarios con el Asistente en Google Home son almacenadas de acuerdo con las Políticas de Privacidad de Google. Esa información está disponible para el usuario y, generalmente, **almacenada hasta que el usuario la borre**", explican desde la compañía.

En este artículo te explicamos cómo hacer que **Google elimine automáticamente cada cierto tiempo tu actividad de búsqueda**. ¿Por qué lo necesitas? Lo que le pidas al asistente de Google se puede luego **relacionar con el resto de productos de la empresa**. En el caso de Alexa, con los pedidos que hagas online a Amazon; en el de Google, para por ejemplo recomendarte vídeos en YouTube.

En el caso de Alexa ocurre lo mismo. Borrar las grabaciones **corre a cargo de los usuarios** y se requiere iniciar sesión en la cuenta de la compañía para configurar el asistente a través de este enlace. En caso de hacerlo a través de la app Alexa, hay que acceder a Ajustes > Privacidad de Alexa. Si no se realiza esta acción manualmente, la compañía no especifica si las borraría después de un tiempo.

¿Y Siri, de Apple? Según la Política de Privacidad de la compañía, analizan "a fondo la necesidad de recopilar los datos de carácter personal y, en caso de que tal necesidad exista" solo conservan los datos "durante el período de tiempo más corto posible para cumplir con el fin para el que se han recopilado".

Para el uso de su asistente de voz, concretamente, el historial de grabaciones se guarda durante seis meses (si no se elimina manualmente) **asociada a una "identidad aleatoria"** para seguir investigando el desarrollo de Siri. Se pueden usar junto a otros datos del dispositivo, como la configuración del móvil o el ordenador, e incluso la ubicación de la persona al hacer una pregunta. A partir de los seis meses, si no los borramos, **se conservan estos datos junto al historial** para estudiar los avances del procesamiento del lenguaje durante dos años. Sobre todo, preguntas y comandos concretos.

Es decir, que **ninguna deja claro el tiempo por el que se conservan las grabaciones**, sino que por defecto es indefinido, hasta que decidimos eliminarlas.

https://maldita.es/malditatecnologia/2020/08/18/asistentes-voz-datos-guardan-borran/

Lo que significa para tus datos que una multinacional tecnológica (Facebook) compre una plataforma que usamos todos (Giphy)

20/05/2020

Facebook ha comprado la plataforma Giphy, que es a día de hoy uno de los sitios web que más animaciones GIF distribuye por Internet. Si alguna vez nos has leído en *Maldita Tecnología* o *Maldita Ciencia,* habrás visto que nos gusta amenizar la lectura con estos **pequeños fragmentos de vídeo**. Incluso cuando usas **WhatsApp, Telegram o Twitter**, verás que tienes una opción para complementar tus comentarios con GIFs de cualquier tema que te imagines. Lo haces de manera gratuita, **también cuando abres una cuenta para crear los tuyos propios**. Ahora Facebook ha comprado a Giphy por **400 millones de dólares**. ¿Te has preguntado qué implicaciones tiene esto para los datos que manejan?

Pensad en el ejemplo de WhatsApp y cuando Facebook la adquirió en 2014. **WhatsApp era y sigue siendo un servicio gratuito**, pero del que Facebook se ha beneficiado por la expansión que hace de sus servicios y la información que recoge de la plataforma. Entonces, pagó **19.000 millones de dólares por la firma de mensajería** (en ese año, unos 14.000 millones de euros). La compañía tiene una familia de empresas, entre ellas Instagram, por ejemplo, con la que intercambia datos sobre cada servicio.

Con este tipo de compras, Facebook se hace con más y más y más información para **aumentar su capacidad de vender publicidad** y de hacer que los anuncios que ves cuando navegas por la plataforma o en otros servicios que trabajan con la red social estén hechos a tu medida. El **98% de los ingresos de Facebook viene de la publicidad**, según su informe anual de datos fiscales (pág.62), y es una compañía que puede ganar en torno a 50.000 millones de euros anualmente (pág.67).

¿Por qué una plataforma que es gratuita le cuesta tantos millones a una multinacional tecnológica?

“La estrategia de Facebook consiste en que cuando le sale un competidor, **su forma de aniquilarlo es comprarlo**: absorbe la competencia y compra la solución”, explica a *Maldita Tecnología* **Liliana Arroyo**, investigadora de innovación digital y su impacto social en la Escuela Superior de Administración y Dirección de Empresas (ESADE). Google, por ejemplo, es dueña de Tenor, **la plataforma que le hace la competencia a Giphy** (y que se usa en WhatsApp).

Estas adquisiciones contribuyen a que Facebook pueda ampliar su conocimiento **sobre su comunidad de usuarios englobando las de otras plataformas que considera potenciales**. Por ejemplo, Facebook ya cuenta con información sobre **quiénes somos, con quién nos relacionamos, qué nos gusta o por donde nos movemos (y más)** gracias a su red social, pero puede ampliar ese espectro viendo qué tipo de contenido compartimos en Instagram, en qué anuncios pinchamos o qué GIFs solemos enviar.

“Al adquirir Giphy, **Facebook obtiene acceso a los datos que Giphy rastrea y puede integrarlos**, a su vez, de forma transversal en todos sus productos. Son muchos datos, y además con **fuerte penetración en un segmento de edad significativo**”, explica **María Lázaro**, profesora de Márketing Digital en distintas universidades y directora de Desarrollo Corporativo del Real Instituto Elcano.

Así, Facebook crea “puntos de contacto diferentes con los usuarios porque con estos puertos de entrada **accede a distintos tipos de público y le permite ampliar segmentos** y conocer más perfiles”, explica Arroyo. A partir de ahí, es más fácil ofrecer mejores datos a sus clientes, es decir, a las empresas que quieren poner anuncios: “Todo esto nos permite unir los **distintos puntos, hacer una radiografía de mayor dimensión** de las personas que usan el ecosistema de Facebook”, continúa.

Los GIFs de Giphy llegan diariamente a unos 700 millones de usuarios diarios entre todos los servicios que ofrece. Según datos de Estados Unidos de Statista, el 28% de sus usuarios tiene entre 18 y 24 años, mientras que el 26% entre 25 y 34 años. “Statista no incluye en su análisis e**l segmento de menores de edad**, los chicos y chicas de entre 13 y 18 años, que conforman un grupo muy representativo entre los usuarios de Giphy, no en vano los GIFs forman parte del **lenguaje común de expresión entre niños y adolescentes**”, señala Lázaro. En teoría, los menores de 13 años no pueden crearse una cuenta en Giphy porque la compañía no lo permite.

¿Qué tipo de datos puede usar una multinacional a partir de una firma más pequeña como Giphy?

Quizás os parezca irrelevante, pero a estas compañías les sirve mucho analizar **el comportamiento que tenemos cuando interactuamos** en sus plataformas. Las **búsquedas** que hacemos en Giphy se analizan, junto al **dispositivo** que utilizamos para hacerlas, el **tipo de imagen** que buscamos y **dónde la colocamos** luego: si en una red social, en un servicio de mensajería… ¿Usamos GIFs graciosos en **nuestros perfiles públicos** o nos da más palo y solamente los pasamos en **nuestras conversaciones privadas** en apps de mensajería? ¿Son tristes o alegres? ¿Sobre qué tema?

Cuando usamos Giphy en otros sitios como Twitter, la compañía se vale de **una serie de rastreadores** para obtener datos sobre **nuestra navegación** en ellos y las imágenes que usamos en esa plataforma, que luego asocia al “perfil” que puede hacer de nosotros. Cuando lo hacemos, **estamos sujetos a sus propias políticas de privacidad**, según la de Giphy. ¿Qué ha hecho por ejemplo Signal, una de las plataformas de mensajería que recogemos en nuestro "Kit de Privacidad"? Hacer una serie de cambios técnicos para que cuando realizas una búsqueda de GIFs en Signal, **parezca que la búsqueda la ha hecho el propio Signa**l desde sus servidores y no nosotros individualmente. De esta manera protege un poco más la identidad de sus usuarios.

“A día de hoy, quizás Giphy no pueda identificar a usuarios o personas que ven sus GIFs de manera individual pero, combinado con los mecanismos de traceo de Facebook, **probablemente se podrá empezar a identificar a usuarios, o al menos relacionarlos con los comportamientos online** que se producen en otros sitios web”, explica a *Maldita*

Tecnología **Mitch Stoltz**, consultor legal de Electronic Frontier Foundation, una de las principales organizaciones mundiales de defensa de los derechos digitales.

Stoltz resalta que **combinar la información que Facebook empiece a derivar de Giphy** con la que ya obtiene del resto de servicios que posee su compañía es ya de por sí una manera de **reforzar su máquina aspiradora de información**. Aun así, Facebook podría emplear nuevos rastreadores técnicos (en este artículo puedes leer más) para que al compartir un GIF se pueda sacar más aún **sobre nuestro comportamiento en Internet**. Es decir, que tú no vas a notar nada en cómo utilizas tus mini-vídeos, pero la multinacional va a tener un nuevo pozo de información que sirve para ampliar sus bases de datos.

"La publicidad personalizada es una *vía importante de beneficio* para Facebook, **pero no la única**: los datos que Facebook recoge **le permiten customizar sus otros servicios**, por ejemplo el tablón que ves en la red social. Esta información también les da inteligencia de mercado: les ayuda a decidir qué compañía comprarán a continuación", dice Stoltz, y con esto seguir **ampliando comunidades de usuarios potenciales** para su negocio.

https://maldita.es/malditatecnologia/2020/05/20/datos-multinacional-tecnologica-facebook-compra-giphy/

El caso de FaceApp: un ejemplo de uso abusivo de datos que se aplica a otras aplicaciones gratuitas

15/06/2020

Antes, la gente quería saber cómo sería cuando llegase a la tercera edad, y ahora quieren verse transformados en el sexo contrario. En 2019, la aplicación para móviles **FaceApp**, de origen ruso, se hizo famosa por lo primero, y ahora que ha añadido una funcionalidad para perfeccionar lo segundo ha vuelto al estrellato, pese a la **polémica que generó el uso maltrecho que le daba a los datos personales** que recogía.

¿Por qué el uso de esta aplicación de forma masiva es relevante? El año pasado, la gente subía fotos suyas, de sus colegas, de famosos… Hasta que se denunció que **las imágenes que subíamos y la información personal que recogía se guardaba en Estados Unidos** y se podía **compartir con empresas en Rusia.** La alarma sonó especialmente por el tema de las fotos personales: podía acceder a nuestra galería o a nuestras redes sociales si le dábamos ese permiso y luego **esa información terminaba en manos ajenas**, sin tener muy claro tampoco lo que se hacía con ella por lo mal que explicaban sus usos.

Políticas de privacidad cuestionables que nadie se lee con tal de participar en un juego viral que nos transforma la cara

El gran problema con FaceApp se reduce a que **en 2019 se viralizó su uso** y por eso se pudo denunciar que su Política de Privacidad avisaba de que guardaban las imágenes que usábamos junto a otro puñado de datos que sacaban de nuestra navegación o nuestro dispositivo. Pero por regla general, **las Políticas de Privacidad y los Términos y Condiciones no se leen**. Si se hiciera, a alguien le podría haber sonado raro que una foto de su cara llegara a Rusia con fines comerciales (u otros que no se especifican).

“Entrenar algoritmos para el reconocimiento de imágenes o para entrenar sistemas de videovigilancia es la opción más razonable de lo que pueden hacer, ya sean propios o incluso para otros, aunque no lo digan”, explica a *Maldita Tecnología* **Jorge Morell**, abogado especializado en tecnología y en Términos y Condiciones.

Con fotos de caras, además, se puede analizar el color del pelo para saber si es tinte o natural y personalizar la publicidad o cosas algo más graves como hacer predicciones sobre si clientes de una aseguradora han sufrido o pueden sufrir obesidad (lo que podría variar el precio de una tarifa), entre muchas otras, como cuenta Morell.

Poco antes de sacar la nueva función para cambiarnos de sexo en junio (antes se podía pero con filtros mucho menos definidos), FaceApp cambió su Política de Privacidad. La antigua puede leerse todavía en una copia y la diferencia es abismal, puede que con la renovada no hubiese saltado tanto la alarma el año pasado. **Han quitado toda referencia a Rusia**, uno de los puntos que más controversia generó el año pasado, y aclarado que **no se usan las imágenes que subimos para otro fin que no sea usar la app**. En la actualización, sin embargo, no señalan de quién es la aplicación o quién la gestiona, así que **tampoco sabes quién guarda esos datos.**

Aun así, recoge una cantidad de datos tremenda **de nuestro dispositivo y también de los sitios por los que navegamos**: qué páginas visitamos más, cuánto nos quedamos en cada una, cuánto nos quedamos conectados, en qué enlaces hacemos click… Con esa información **también se puede sacar dinero** a través de la publicidad.

“El problema de base es que **no tenemos capacidad de elección**: como no tienes ninguna capacidad de negociar lo que te ponen sobre la mesa, no se le presta ninguna atención” cuando se nos pide hacer click en la cajita de “Acepto la Política de Privacidad”, dice Morell.

FaceApp es el ejemplo perfecto de lo que pasa continuamente con apps gratuitas que recaban datos sin que lo sepamos

En realidad, el caso de FaceApp es un ejemplo perfecto para ilustrar cómo un detalle tan tonto como subir una foto nuestra para vernos con unos años más encima desemboca en que **demos cientos de puntos de datos sobre nosotros a compañías que ni sabemos dónde están** ni lo que hacen con ellos luego. Pero no es más que eso, un ejemplo, ya que muchas aplicaciones gratuitas que usamos vienen con este riesgo.

Un estudio publicado a comienzos de 2020 por el Consejo de Consumidores de Noruega usa diez apps populares (entre ellas Grindr, Tinder o My365, una app de ovulación) que muestra precisamente la cantidad de información que compartimos con ciertas aplicaciones **para que luego estas se compartan con empresas ajenas que los usan con fines comerciales**. Desde la ubicación a la edad, la orientación sexual, pasando por nuestra percepción política, cuando menstruamos o incluso si consumimos drogas.

“Cualquier consumidor con un promedio de aplicaciones instaladas en su teléfono -entre 40 y 80 aplicaciones- es susceptible de que se hayan compartido sus datos con **cientos o quizá miles de actores online**”, afirmaba el director del estudio, Finn Myrstad, a *The New York Times.*

El estudio asegura que muchas de las aplicaciones gratuitas que usamos tienen una “base legal cuestionable para recolectar y usar datos de los consumidores”. ¿Por qué? Porque o bien **no nos especifican para qué se van a usar los datos** que recoge de la aplicación que estamos usando o porque **lo esconde dentro de la política de privacidad** para que no logremos entender qué es lo que quieren hacer con ellos.

“Los Términos y Condiciones son documentos de derechos y obligaciones de uno y otro, son contratos, lo que pasa es que **la sensación de firmar es tan inocente que parece que es algo irrelevante**, pero es una irrelevancia que en el corto plazo no va a tener mucho efecto y en el medio o largo plazo, cuanto más estés en una plataforma, más impacto puede tener”, asegura Morell.

https://maldita.es/malditatecnologia/2020/06/15/faceapp-uso-abusivo-datos-aplicaciones-privacidad/

‘30 euros de regalo por apuntarte, luego si quieres te das de baja’: trucos de fidelización para liarte o recabar datos

27/05/2020

Seguro que más de una vez te has apuntado a **alguna promoción** o te has comprado algo que necesitabas aprovechando un fantástico descuento que, aparentemente, **no te cuesta nada**. “Con esta promoción, te dan 30 euros de regalo sólo por apuntarte, **luego si quieres te das de baja**” o “hazte socia para recibir **descuentos exclusivos** antes que nadie” son frases que has tenido que escuchar sí o sí estando de compras o visto en alguna publicidad.

Si de primeras es **gratuito** y además se pueden sacar beneficios como una devolución de dinero o descuentos prolongados a lo largo del tiempo y exclusivos, **¿dónde está el truco?** La mayoría de las veces en la confianza de que la gente **olvidará que está suscrita a una promoción** que terminará por costar más de lo que parecía, pero también en la **letra pequeña** de lo que estamos firmando y los datos personales que estamos otorgando.

¿Por qué nos piden darnos de alta en servicios online a cambio de recompensas?

Muchas veces estas ofertas y promesas de descuentos se fraguan mediante un **contrato digital** o se **aplican a un servicio online.** Son parte de las estrategias de marketing para fidelizar clientes que crean las empresas y que pueden darles beneficios directos de varias formas, entre ellas las que os hemos mencionado: **aprovechar el paso del tiempo y que olvidemos nuestra suscripción** (sumado a la dificultad para darnos de baja) y la **colección de datos personales** con los que pueden hacerse durante un tiempo determinado.

Pongamos un ejemplo concreto para ilustrar todo esto: a principios de 2020 una cadena que vendía productos electrónicos inició una promoción que consistía en **la devolución de 30 euros del total de tu compra ‘solamente’ por apuntarte a una suscripción** de un servicio de seguros. Resulta que cuando aceptabas, la suscripción ya no sólo era a un seguro, sino también a un servicio de *cloud*, para guardar archivos en una nube. Las **cosas gratis no paraban ahí**, sino que también te regalaban una página web, con el dominio a elegir.

¡Cuántas cosas gratis! ¿Y todo por suscribirme? ¿No hay que hacer nada más? **Aparentemente, no**. "Los 30 euros llegan seguro, eh, yo lo hice y me llegó a las 4-6 semanas sin problema", decía una empleada en su momento para convencer que se completara el proceso. **Al llegar a este punto, con cualquier promoción, desconfía.** O, al menos, **asegúrate de cuáles son las condiciones exactas a las que está**s accediendo.

En este caso concreto, lo que se aceptaba era iniciar un pago mensual para pagar un seguro para el producto electrónico adquirido más el servicio de *cloud*. El primer mes era gratuito y a partir de ahí se pasaba a **pagar una cuota para cada servicio** (la más alta que ofrecían, que entre los dos servicios llegaba a los 40 ó 50 euros). Los 30 euros de descuento ya no parecen tan gratuitos, ¿verdad?

El truco en todo esto está en que el cliente no sea del todo consciente de que en realidad está contratando un **servicio mensual que tendrá que dar de baja** o mínimo gestionar para no tener que pagar la cuota más elevada. Si se optaba por darse de baja del servicio, se avisa de que los 30 euros de la promoción no llegarán, pero la transacción está hecha y ambas empresas ya cuentan con **un buen pellizco de datos del consumidor**: nombre apellidos, dirección postal, dirección de correo electrónico, número de teléfono, identificación bancaria y número de cuenta y tipo de producto que se ha comprado. Toda esa información por un servicio que **ni siquiera has llegado a utilizar.**

Por eso, cada vez que accedas a participar en un programa de este tipo, es importante que **leas los términos del servicio** que estás firmando. Normalmente, vendrán en contratos de muchas páginas y letra pequeña. A eso habrá que sumarle la **Política de Privacidad y las Condiciones de Uso** para saber con qué garantías van a tratar tus datos.

¡La letra pequeña!

Jugar con la **memoria de las personas** y con la incapacidad de leerse todos los **interminables documentos sobre condiciones de uso y datos** es algo que las empresas (sobre todo las tecnológicas) hacen continuamente. Un ejemplo de esto son las **operadoras de telefonía** y los contratos de promociones y tarifas más baratas. Quizás te haya pasado alguna vez que al contratar un servicio a un precio supuestamente fijo te hayas llevado una sorpresa al llegar la factura. O que pactaras un precio, y dos años después se termina ese contrato y la factura de repente se ha duplicado.

Estos casos son extrapolables a muchos otros servicios, empresas y promociones. Algunas buscarán liarnos para que **terminemos pagando una suscripción mensual** y quizás nos cueste darnos de baja. Otras simplemente querrán **conocernos más como clientes para conseguir vendernos más cosas** y eso lo harán pidiéndonos nuestros datos y dándonos pequeñas recompensas para que acudamos más veces. Las tiendas de ropa, por ejemplo, tienen ese tipo de programas de fidelización.

Hace poco os dimos algunas pistas y consejos para deshaceros de las cuentas que hubieseis abierto para, por ejemplo, este supuesto y **que ya no uséis**: recibir promociones o comprar algo más barato de lo habitual gracias a un programa de fidelización. Puedes leer más en este artículo. Sin embargo, la mejor prevención es **estar atento a las condiciones que nos piden**, los documentos que estamos firmando y la letra pequeña.

https://maldita.es/malditatecnologia/2020/08/14/regalos-promociones-trucos-fidelizacion-liarte-recabar-datos/

Homescapes y otros llamamientos a juegos gratuitos en redes sociales que te enganchan a ti y a tus datos

27/06/2020

A muchos de vosotros os salen anuncios en vuestras redes sociales de **juegos gratuitos que enganchan hasta decir basta**. Uno que aparece recurrentemente es el de Gardenscapes o el de Homescapes, de la familia de juegos de Playrix, y que llevan ya más de 100 millones de descargas en Android. No hay mejor ejemplo para contaros que estos juegos **son gratuitos y de ahí que puedan sacar beneficios de otros sitios**. ¿Por ejemplo? De la información personal que obtienen sobre sus usuarios.

Esto no quita que sea una **práctica legal**, ojo. Estas aplicaciones tienen políticas de privacidad que **avisan de que recogen una cierta cantidad de datos** de nuestra experiencia de juego y nuestros dispositivos para luego colocar publicidad en él o en otros servicios. De modo que al descargarlos y jugar, **estamos dando nuestro consentimiento** a que se recojan con un objetivo normalmente marcado: los perfiles publicitarios.

Todo sirve: desde el sitio desde el que juegas a cuánto tiempo pasas jugando

Cuando descargas y comienzas a jugar en una aplicación así, puedes hacerlo **consciente o no de que va a recoger cierto tipo de datos** Obviamente, van a querer saber cómo avanzo en el juego, ¿no? Si paso de niveles, si compro cosas, si juego con alguien o solo... Todo con la idea de **mejorar nuestra experiencia en el juego**.

La familia de juegos de Playrix guarda datos de lo que le damos conscientemente **al empezar a jugar o registrarnos**: email o nombre o nick y los comentarios o mensajes que mandes. A la vez, registran el **tipo de dispositivo** desde el que nos conectamos: si es un ordenador u móvil, de qué marca, la dirección IP, el idioma y activa diferentes rastreadores y por supuesto cookies. A grandes rasgos también saben **dónde nos encontramos físicamente** (eso si no concedes acceso directo a la geolocalización).

Si accedes a través de Facebook o Google o una vez iniciado el juego te conectas a una red social, la empresa también puede obtener datos como **tu email, tu nombre en la red social y también tu foto de perfil**, de modo que ya te pone cara aunque utilices un nick falso. Muchas aplicaciones y juegos se conectan de esta manera.

En el caso de este juego concreto, lo pide constantemente mientras vas jugando. Incita a hacerlo con **regalos y promesas de vidas extra** o recompensas con la premisa de formar "comunidades" pero, por norma general, el acceso a tus redes sociales es más valioso.

Otro de los factores clave de leer la Política de Privacidad de este tipo de juegos es que a pesar de anunciarse en redes sociales como Instagram o Facebook, pueden tener límite de edad de uso. En este caso concreto, **si eres menor de 16 años no puedes usar el juego**, pero es muy probable que la mayoría de adolescentes que puedan jugar a él no lo sepan y, sin embargo, la compañía en cuestión **ya cuenta con cierta información**.

Un modelo de negocio probado para las aplicaciones y juegos gratuitos

Por norma, la mayor parte de los juegos gratuitos y aplicaciones similares hacen recopilaciones ingentes de datos personales **con fines de márketing**. Su **modelo de negocio** se puede asemejar con **una gran fábrica donde los usuarios somos los trabajadores**: entramos cada día a ella a producir contenido e interacciones que van desde los 'me gusta' y las cosas que compartimos a las cosas que se cogen sin que lo sepamos, como los rastreadores y a lo mejor nuestra ubicación.

Ahí entra en juego **la tecnología que no vemos**, los sistemas que lo organizan todo. Uno de los estudios que describen este modelo lo cuenta tal cual: "La materia prima principal en el proceso **(los datos, el contenido y los metadatos)** son los objetos de trabajo y **están creados por humanos**, pero el trabajo en sí en realidad **lo llevan a cabo algoritmos**".

Toda esa "producción" que nosotros hacemos a través de las aplicaciones y las redes sociales que frecuentamos la analizan sistemas automatizados hasta formar **paquetes de datos que van asociados a mi persona** y que pasan por distintas fases de distribución al salir de la fábrica. ¿Dónde llegan a parar? Normalmente, a los **data brokers**, las compañías intermediaras de las que te hablamos aquí, que luego los venden a otras empresas.

La fábrica, además, nunca para. Nuestros gustos y nuestra forma de interactuar con aplicaciones y redes sociales **van cambiando** y eso también se tiene en cuenta. Otro gran estudio publicado en 2020 sobre este modelo de negocio en aplicaciones **habla directamente de consumidores "explotados" por la industria publicitaria**.

¿Que a dónde vamos a parar con todo esto? A que en efecto, el **modelo económico actual basado en nuestros datos personales es extremo** y ganar conciencia de la información que regalamos continuamente a las compañías es vital para hacer un uso responsable y sano de la tecnología.

Descargar un juego gratuito para entretenernos no está mal siempre y cuando seamos conscientes de que al hacerlo **estamos cediendo una parte de nuestro información personal** que hace que la fábrica siga en funcionamiento **para que se beneficien todo tipo de empresas**, y que en algunas ocasiones lo que nos piden va a ser **más abusivo** que en otras.

https://maldita.es/malditatecnologia/2020/10/06/juegos-gratuitos-anuncios-redes-sociales-enganchan-datos/

Crowdless y otras aplicaciones colaborativas: cómo se usan y guardan los datos

03/07/2020

Nos habéis preguntado por una aplicación en particular llamada Crowdless, pero vamos a tratar de daros una respuesta que podáis usar en general al usar servicios digitales. Al final, la mayor parte de la preocupación por la privacidad **se resuelve con una medida relativamente sencilla** (aunque tediosa, que lo sabemos): **leer los Términos y Condiciones y la Política de Privacidad** de los sitios.

Crowdless es una aplicación lanzada en abril que sirve para comprobar en tu zona geográfica qué locales y espacios públicos están más concurridos que otros. La iniciativa surgió **a cuenta de la pandemia del coronavirus** y la necesidad de mantener el distanciamiento social y recoge los datos de servicios como **Google Places o Google Maps** (que ya hacen esto para servicios como el transporte público).

Puedes ser "voluntario" en la app, que implica participar en acciones que van desde **apuntar tu local para registrar la concurrencia a añadir comercios** y espacios que no están en ella. Este tipo de aplicaciones colaborativas son muy comunes y cada una tiene sus particularidades. Por ejemplo, con la COVID-19 surgieron varias **para que la sociedad "colaborase" con el control de los contagios,** por ejemplo apuntando si tenían síntomas, pero a la Agencia Española de Protección de Datos (AEPD) no le gustó demasiado la idea por los riesgos a la hora de mover datos de salud.

En el caso de Crowdless, su Política de Privacidad no dice mucho de lo que hacen con nuestra información, lo cual no es un punto a favor. Desde la compañía, explican a *Maldita Tecnología* que **no recogen datos personales de gente que usa la app**, pero que sí pueden guardar la información de personas que "rellenan encuestas, formularios o se **apuntan a programas como el de los voluntarios**".

Explican que esa información personal se guarda en una "base de datos encriptada" a la que solo puede acceder la compañía, que esos datos **sólo se guardan para comunicarse con los voluntarios** y que no se comparten a terceros. Esta información no está especificada en su política de privacidad, que es lo que cuenta.

Este caso puede servir como patrón para muchas otras aplicaciones que **nos vamos a encontrar que sean poco específicas en sus textos de privacidad**: "Hay que leer siempre las políticas de privacidad de las apps móviles, y en caso de que sean o escuetas o no te den confianza **quizás mejor no utilizarlas**", explica Jorge Campanillas, abogado especializado en protección de datos y comunicación.

Deja a elección de cada consumidor que delibere entre usar una aplicación opcional: "Todas las aplicaciones pueden ser inocuas, **pero no lo sabemos a ciencia cierta**", dice este abogado. Además, dado que las plataformas tienden a **"no siempre ser lo transparentes que les exige la normativa", nos generan dudas** y eso es normal. Lo mejor es "utilizarlas con cuidado o **preguntar directamente a la compañía**, a ver qué tipo de respuesta dan a la consulta para dejarnos totalmente tranquilos".

Por su parte, Camino García, abogada especializada en derecho digital, señala que la Política de Privacidad de esta aplicación es **“incompleta” e “insuficiente”** porque no ahondan en el sistema de registro que tienen ni especifican “para qué se utilizan los datos, durante cuánto tiempo, los destinatarios a los que, en su caso, se comunicarán los datos o cuál es la base legal del tratamiento”, **puntos clave** de un documento así.

Contando con que no siempre es posible hacer un análisis desde una perspectiva legal de una Política de Privacidad, lo ideal según estos profesionales es **usar las aplicaciones con cabeza** (es decir, no descargar ochenta en nuestro móvil por el mero hecho de tenerlas), **analizar su objetivo** y en función de ello y de lo que podamos observar en su funcionamiento y sus documentos legales **pensar si nos hace falta y vale la pena**. ¡De modo que todo el mundo a hacer limpieza de aplicaciones!

https://maldita.es/malditatecnologia/2020/10/04/crowdless-aplicaciones-colaborativas-como-se-usan-guardan-datos/

Qué es la 'privacidad por diseño' y por qué es importante

02/10/2020

Desde que se puso en marcha la aplicación Radar COVID para rastrear contactos de personas contagiadas, ha salido a colación el término **"privacidad por diseño"**, ya que la tecnología en la que está basada (te hablamos sobre ella aquí) sigue este principio. ¿Qué significa que la "privacidad" esté en el "diseño" de una tecnología y por qué es importante?

El *privacy by design*, como se conoce en inglés, es una iniciativa en la que hacen hincapié tanto organizaciones que trabajan por un **uso cívico de la tecnología**. Está dirigida a la **parte previa a la elaboración y presentación de un servicio**, como una app o una red social, por lo que también actúa como un "principio" que puede seguir una compañía.

Lo que busca es centrar los primeros pasos del diseño de ese servicio en desarrollar políticas que **sitúen la privacidad y la protección de los datos de los usuarios por delante.** Es decir, que estos factores sean los que primen a la hora de construir una app, por ejemplo, y no el beneficio propio de la compañía o institución que lo hace.

Un servicio o aplicación que se base en este principio **no podría explotar tu información personal** para enriquecerse ni venderla para fines que no conoces, a diferencia del modelo de negocio basado en datos que predomina ahora. Aquí te contamos el ejemplo de FaceApp o de otras aplicaciones que lo siguen.

¿Para qué? Pues para evitar cosas como las brechas y fugas de datos, que la empresa propietaria venda tu información a otras empresas, que el diseño sea algo más seguro ante ataques informáticos, etc. Pero principalmente, el objetivo es asegurarse de que las entidades que crean servicios tecnológicos **respeten la privacidad de sus usuarios y conviertan esta práctica en algo habitual**.

El concepto no es algo que haya surgido ahora que interactuamos diariamente con un smartphone y todas las aplicaciones, servicios, redes sociales, etc. que incluye. Lo planteó en la década de los 90 una investigadora canadiense llamada **Ann Cavoukian** y que a día de hoy es referencia en el campo de la privacidad y la tecnología. ¿Por qué hacía falta entonces, cuando el acceso a Internet no era tan masivo? Cavoukian explica que los efectos de las Tecnologías de Información y Comunicaciones (TIC) serían imparables y que la conectividad que traerían a las personas requeriría de estas protecciones.

En el caso de la tecnología en la que está basada la app Radar COVID, llamada **DP3-T**, ha sido desarrollada para que pueda funcionar garantizando el anonimato: móviles pueden conectarse entre sí para enviarse códigos que **no pueden identificar a sus propietarios**.

https://maldita.es/malditatecnologia/2020/10/02/que-es-privacidad-por-diseno/

"WhatsApp está usando Micrófono": ¿sabes cuáles son todos los permisos que concedes a las apps de tu móvil?

09/03/2020

Quizás te suena haber visto una pequeña referencia a los permisos de una app al descargarla de una tienda virtual como la Play Store en el caso de tener un dispositivo Android. O quizás no, y por eso te interesa lo que contamos aquí.

Los permisos de las aplicaciones son aquellos **accesos que otorgas a una app para que pueda funcionar bien cuando la instalas**. Por ejemplo, que Cabify pueda acceder a tu ubicación para que el conductor sepa dónde recogerte cuando pides el servicio.

Una app puede pedir que le des acceso al **almacenamiento de tu móvil, al calendario, los contactos, la cámara y el micrófono, los SMS, la ubicación y hasta a sensores corporales**, entre otros. Son los que se consideran más "delicados" por temas de seguridad del usuario. La cuestión es que **unos pueden ser necesarios para que la app funcione, pero otros no.** Por ejemplo, Twitter puede pedirte acceso a la cámara y al contenido multimedia para que puedas compartir una foto, pero es algo más raro que una app de Mapas necesite acceso a enviar SMS desde tu móvil para funcionar.

Entonces, ¿para qué iba a pedir una aplicación muchos permisos a la vez? ¿Por qué son tan valiosos los datos que se obtienen a partir de estas funciones del móvil? "Por sus características y que lo llevamos constantemente con nosotros, **los smartphones son los mejores medios para datificar nuestro entorno y comportamiento diario** y hacer un mejor perfilado de quienes somos y cuáles son nuestros hábitos de consumo", explica a *Maldita.es* Carlos Fernández Barbudo, doctor en Ciencias Políticas e investigador sobre la relación de la tecnología y la privacidad.

"Normalmente, los desarrolladores de apps más sencillas [como la de una linterna] usan toda esa información que están captando a través de permisos para vendérsela a data brokers, **es una cadena de suministro**", continúa Fernández Barbudo. Esto no se hace tanto a nivel individual como en **paquetes grandes de datos de determinados perfiles:** es como si el que desarrolla la app tuviese un campo de patatas, lo que realmente le interesa es vender la patata al por mayor, darle salida aunque sea más barato. "Luego son otros agentes los que empaquetan y dan forma", concluye.

Si no doy esos datos voluntariamente, ¿tienen que pedirme permiso para recogerlos usando funciones de mi móvil? Pues depende de cómo venga especificado. Para empezar, los objetivos por los que se quiere recopilar ciertos datos **tienen que estar incluidos sí o sí en la Política de Privacidad** de una aplicación.

"Si no fuera el caso y el micro/cámara/otro sensor fueran un elemento muy accesorio a la finalidad principal de la app (por ejemplo una calculadora que quiere grabar un audio o tu geolocalización), podría bastar que el tratamiento se indicara en la Política de Privacidad pero **por defecto no debería estar activado su uso** y se debería **pedir permiso al usuario** para su puesta en marcha", explica Jorge Morell, abogado especializado en protección de datos y autor del blog Términos y Condiciones.

Según el principio de minimización de datos del art. 5.1 c) del Reglamento General de Protección de Datos y el art. 25 relativo a la privacidad desde el diseño y por defecto, los propietarios de las aplicaciones **no deberían obligar a los usuarios a aceptar prestaciones que no son necesarias para que funcionen**. Es decir, que la app de mi periódico no puede dejar de funcionar por que no le de acceso a mis contactos.

No limitar los permisos que le das a una app es como dejar el coche en el parking sin cerrar: **una puerta abierta a que los propietarios de la aplicación cojan más datos de los que debieran**. Lo ideal es que los que no sean estrictamente necesarios estén siempre desactivados y que si necesitan activarse se hagan de manera puntual. Así nos evitaremos cuestionarnos por qué de repente WhatsApp está usando el micrófono si no tengo la app abierta en el móvil.

Las últimas versiones de Android (vamos por la versión 10) garantizan que cuando por primera vez una app vaya a pedir acceso a un permiso que considera delicado (como la Cámara o los Contactos, como hemos puesto arriba), nos pedirá autorización. Sin embargo, **una vez que esté dado, se quedará dado**, o sea que si queremos desactivarlo lo tendremos que hacer de forma manual en el menú de Aplicaciones, en Ajustes.

Concretamente, la versión 10 ya permite que demos acceso solo cuando la app se vaya a usar y no en todo momento. Los teléfonos de Apple también funcionan de esta manera. En el menú de Configuración aparece una lista de todas las apps instaladas y en cada una los permisos concedidos. Este sistema da la opción de activarlo solo en momentos concretos.

https://maldita.es/malditatecnologia/2020/03/09/whatsapp-microfono-permisos-apps-movil/

La huella para acceder a apps del banco: ¿el dato biométrico se lo queda el banco o el móvil?

09/07/2020

A la aplicación para móviles del banco se puede acceder con un código pin, que es la opción por defecto, pero **muchas permiten ingresar usando la huella dactilar.** De ahí ha surgido la siguiente duda que nos habéis hecho llegar: ¿esa huella la guarda el banco en cuestión o nuestro dispositivo? Los datos biométricos son **especialmente sensibles** debido a la manera inequívoca que tienen de identificarnos, y tienen que **guardarse y tratarse con mayor cautela** que el resto de información.

Hemos consultado las políticas de privacidad de algunas entidades bancarias para comprobar que **especifiquen el tratamiento de este dato o no**. En el caso de Caixabank, por ejemplo, hablan de la huella dactilar directamente en su Política de Privacidad para avisar de que al registrarla en la app **autorizamos al banco a crearla y guardarla** en sus ficheros. Según el documento, guardan la huella **hasta que termina la contratación de sus servicios** y se usa, principalmente, a efectos de autenticación del cliente.

“El patrón biométrico se ha protegido mediante la aplicación de **varios algoritmos de cifrado**; en ningún caso será posible la reconstrucción de la huella digital a partir del patrón biométrico obtenido”, aseguran en la política.

BBVA también habla de la huella dactilar en su Política de Privacidad, pero esta vez para explicar que, en caso de utilizarla, **se quedará encriptada en tu teléfono móvil** (por lo que la seguridad del patrón biométrico queda sujeta al diseño de cada fabricante): “Esta funcionalidad técnica no es controlada por BBVA y depende exclusivamente del fabricante del dispositivo”.

Hay muchas otras aplicaciones bancarias que permiten el uso de la huella dactilar para autenticarse o completar transacciones pero que **no incluyen esta función en su Política de Privacidad porque no la tratan** directamente (se guarda en el dispositivo).

Hemos preguntado al Banco Santander por este tratamiento y nos confirman esto último: “El Banco no realiza ningún tratamiento de datos biométricos de clientes a través de sus aplicaciones informáticas, sino que las funciones de identificación y autenticación, mediante el uso de tecnologías de huella digital o reconocimiento facial, **las realiza el sistema operativo del dispositivo móvil del usuario**”, asegura un portavoz.

En el caso de Bankia, más de lo mismo: esta información no aparece en la Política de Privacidad de la app sino en el Aviso Legal, otro documento legal obligatorio. El sistema de identificación no lo facilita ni lo gestiona Bankia, sino el fabricante del dispositivo móvil.

Los móviles tienen funciones específicas para guardar datos biométricos como la huella dactilar

Hablando en términos técnicos, las funciones de identificación y autenticación a través de datos biométricos se llevan a cabo mediante **capas de software que implementan los**

propios sistemas operativos. En cada dispositivo, ya sea de Android (Google) o de iOS (Apple), se localiza una especie de caja fuerte donde se **guardan datos como el de la huella dactilar.** Un banco como Santander no recibe el dato en sí, sino una clave de acceso a la caja, que la **vincula con la aplicación**, y que valida que lo que hay dentro es mi huella.

Este informe del INCIBE de 2016 señalaba que una de las principales vulnerabilidades del uso de la huella dactilar es la "aceptación de muestras biométricas falsas como fotografías, dedos de goma, etc." que permitiría **una autenticación falsa al usarla o llevar a la suplantación de identidad**. Además, desde la implantación del Reglamento General de Protección de Datos (RGPD) en 2018, esta categoría de datos tiene una protección especial (Artículo 9).

https://maldita.es/malditatecnologia/2020/07/09/huella-apps-banco-dato-biometrico-movil/

¡Mamá, papá, soltad ya esa cámara! Los riesgos de compartir imágenes de menores en Internet

23/10/2020

Nos habéis preguntado por un tema que se lleva discutiendo años, desde que entraron en escena las redes sociales. O sea, **más espacios a los que subir fotos y vídeos de bebés** (porque cómo te vas a resistir a esos mofletes o a compartir sus primeros pasos con todos tus amigos a la vez) y menores. Sin embargo, aún tenéis preguntas: ¿qué supone para un menor que subamos sus imágenes mientras son pequeños? ¿Interfiere con su derecho a la privacidad? ¿Pueden ellos de mayores pedir que se eliminen esas fotos?

Este fenómeno tiene un nombre que hemos cogido prestado del inglés: ***sharenting***. El término mezcla las voces inglesas '*share*' (compartir) y '*parenting*' (criar a los hijos), así que ya podéis ver por dónde van los tiros. Resume la costumbre que tienen los padres y familiares de **subir fotografías y vídeos de sus hijos a las redes sociales y compartirlas a través de aplicaciones** como WhatsApp como si no hubiera un mañana.

"Puede parecer que compartir una o varias fotos 'graciosas' de nuestro hijo/a en un grupo de mensajería familiar o en nuestro perfil de redes sociales, es un gesto inocente que no tendrá mayor repercusión. Pero **es un contenido sensible por el mero hecho de afectar a la imagen de un menor**, y pasa a formar parte de una cadena de difusión de información", explican en esta publicación de la campaña *"Internet Segura For Kids"* (IS4K) del INCIBE.

Es decir, que no debemos pensar que por que colguemos una foto en nuestro perfil personal de una red social o la compartamos en un grupo de conocidos, **esas imágenes no pueden acabar en el ordenador de un desconocido** o en el móvil de amigos de nuestros amigos.

¿Y qué tiene esto de peligroso? Los efectos más graves son los casos de suplantación de identidad, de ciberacoso y de *grooming*: **adultos que puedan usar imágenes de esos menores para hacerse pasar por ellos** y establecer relación con otros niños o adolescentes. Hay un momento en el que se puede perder el control de lo que los jóvenes hablan con ellos y les comparten, lo que en un caso extremo **puede derivar en un caso de abuso infantil o chantajes sexuales**. Esto puede ocurrir en el plano online pero también pasar al mundo offline y causar serios problemas de ansiedad a los menores.

"Hay que plantearse si nuestro hijo o hija en un futuro **puede llegar a tener algún problema con esas imágenes**, otro punto es si con ellas estamos creando un **conflicto en la pareja**, en caso de que la otra parte tenga otros criterios al respecto de la privacidad de su hijo/a. También hay que **pensar en su futuro** y si en algún momento esas imágenes pueden **servir para ridiculizar al menor**", cuenta Jorge Flores, director de la organización Pantallas Amigas, dedicada a la alfabetización digital de menores.

Todos en algún momento nos hemos cruzado con un meme viral y nos hemos reído de él, ¿pero qué efecto tendría en ti si fuera tu hijo o hija quien apareciese en él? En este artículo sobre TikTok recogemos cómo desde el INCIBE nos hablaban que incluso revelar la

ubicación de un menor podría llevar a que se produjese daño físico o un problema relacionado con el acoso infantil.

“Especialmente durante sus primeros años de vida, estos no tienen conocimiento ni capacidad de disposición **sobre la sobreexposición a la que se ven sometidos en redes por parte de sus padres**, quienes crean una huella digital del menor prácticamente desde el momento de su nacimiento”, describe a *Maldita Tecnología* Camino García, abogada especializada en privacidad y protección de datos en MRK Abogados.

García incide en que la publicación de fotografías de menores normalmente está asociada a momentos íntimos que se tienen en casa o que los adultos han decidido que son graciosos o importantes, pero sin tener en cuenta que subirlas **puede suponer una intromisión en su privacidad** y que implica estar tomando **una decisión que ellos no han adoptado**. Este hecho tiene mención en el artículo 84 de la Ley Orgánica de Protección de Datos.

La aparición de los *smartphones* fue decisiva **para que se hablara de esta práctica como un fenómeno a tener en cuenta**, ya que nos puso una cámara más o menos potente y un aparato con un espacio de almacenamiento considerable y **conexión a Internet** en el bolsillo sin mayor esfuerzo. Por eso, entre las recomendaciones que da la campaña de IS4K también está la de hacer una reflexión sobre ese panorama: muchos de los servicios que nos animan a subir más y más contenido buscan precisamente que “hagamos pública cada vez más información”. Las empresas también tienen sus propios intereses.

Otra de las preguntas que nos habéis hecho es si los menores de edad pueden pedir que se retiren las imágenes una vez se hagan mayores. Ni siquiera tienen que esperar a cumplir los 18: “En España **la edad a la que los menores pueden prestar su consentimiento para el tratamiento de los datos se fija en 14 años**, por lo que a partir de esa edad podría solicitar la retirada de contenidos, por no haber prestado su consentimiento inequívoco para la publicación de sus imágenes”, nos explica Camino García.

En este artículo de IS4K y esta campaña de Pantallas Amigas y la Agencia Española de Protección de Datos podéis leer algunas claves para reducir el riesgo de la sobreexposición de los menores, como optar por canales no conectados a Internet para compartir fotos (o crear un álbum, por ejemplo) o no mostrar directamente la cara de los peques.

https://maldita.es/malditatecnologia/2020/10/23/mama-papa-soltad-camara-riesgos-compartir-imagenes-menores-internet/