RITSI

Privacidad y datos

Reunión de Estudiantes de Ingenierías
Técnicas y Superiores en Informática

Contenido

1. Política de privacidad y protección de datos en Europa

1.1. Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos

La Carta de Derechos Fundamentales[1] de la Unión Europea establece en su artículos 8 que los ciudadanos de la Unión tienen derecho a que se protejan sus datos personales:

Article 8. Protection of personal data

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

Reglamento 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[2].

Entre sus artículos destacamos:

Capítulo II

Artículo 5. Principios relativos al tratamiento

1. *Los datos personales serán:*
    a. *Tratados de manera lícita, leal y transparente en relación con el interesado*
    b. *Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*
    c. *Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*
    d. *Extractos y, si fuera necesario, actualizarlos [...]*

[...]

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[2] https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Artículo 6. Licitud del tratamiento

1. *El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
    a. *El interesado dio su consentimiento para el tratamiento de sus datos personales (…)*
    b. *El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*
    c. *El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*
    d. *El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física*
    e. *El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (…)*
    f. *El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (…)*

Artículo 9. Tratamiento de categorías especiales de datos personales

1. *Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.*

1.2. Ley de Protección de Datos

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[3] tiene como objeto adaptar el ordenamiento jurídico español al Reglamento 2016/679, el cual hemos mencionado anteriormente.

Si nos metemos en la página web de la Agencia Española de Protección de Datos[4], concretamente en el apartado Ejerce tus derechos[5], nos dicen lo siguiente:

[3] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
[4] https://www.aepd.es/es
[5] https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

"*La normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas*"

2. Política de protección de datos en Estados Unidos

Hasta este año, en Estados Unidos no existía una legislación federal que proteja los datos de los usuarios y la privacidad, es decir, no existe nada similar al Reglamento General de Protección de Datos (RGPD) o a la Ley Orgánica de Protección de Datos (LOPD), sino más bien al contrario: existen normativas sectoriales que regulan diferentes ámbitos como puede ser la Ley de Protección de Privacidad de Menores (COPPA[6]), la Ley de Transferencia y Responsabilidad del Seguro Médico (HIPAA[7]) o la Ley de Cumplimento Fiscal de Cuentas en el Extranjero (FATCA[8])

Fue el 1 de enero de 2020 cuando, en California, entró en vigor la ley de Privacidad del Consumidor (CCPA[9]) que prevé que, si una empresa compra o vende datos de al menos 50.000 residentes de este estado en un año, o sus ingresos anuales superan los 25 millones de dólares, o el 50% de sus ingresos provienen de la venta de información personal de sus clientes, tiene que revelar qué categorías de datos está recopilando y qué está haciendo con los datos de sus clientes.

Además de esto, los consumidores también pueden solicitar a aquellas empresas vinculadas por la CCPA que eliminen todos sus datos personales.

¿Creéis que Estados Unidos debería implementar urgentemente una legislación nacional sobre privacidad de datos? ¿Creéis que la inexistencia de esta reglamentación nos afecta al resto de usuarios del mundo?

[6] Chindren's Online Privacy Protection Rule
[7] Health Information Privacy
[8] Foreign Account Tax Compliance Act
[9] California Consumer Privacy Act

3. Recogida de datos e intercambio entre empresas y actuación del gobierno al respecto

3.1. Cambridge Analytica y Facebook

El caso más sonado en los últimos años acerca de la recolecta masiva de datos con la empresa Facebook de por medio es el caso de Cambridge Analytica[10].

En 2018 salió a la luz que la consultora Cambridge Analytica adquirió de forma indebida información de 50 millones de usuarios de Facebook en Estados Unidos, datos que fueron supuestamente utilizados para manipular psicológicamente a los votantes de las elecciones de 2016, donde Donald Trump resultó electo presidente.

Supuestamente, un profesor de la Universidad de Cambridge llamado Aleksandr Kogan desarrolló en 2013 un test de personalidad que posteriormente respondieron unos 265K usuarios, cediendo permisos para acceder a información personal y a su red de amigos. Fue así como, supuestamente, Kogan se hizo con datos privados (incluidos mensajes) de alrededor de un 15% de la población estadounidense, datos que posteriormente vendería a la consultora.

¿Creéis que es ético, en algún caso, utilizar datos extraídos de RRSS u otros medios para manipular el comportamiento de la población? ¿Utilizaríais estos métodos para algún otro fin que fuese "beneficioso" a nivel nacional o global? ¿Consideras ética la recolecta de cualquier tipo de información si el fin está justificado?

3.2. La Agencia Española de Protección de Datos vs WhatsApp y Facebook[11]

En 2018, la AEPD declaró que las empresas WhatsApp y Facebook habían incurrido en dos infracciones graves de la Ley Orgánica de Protección de Datos:

- A WhatsApp por comunicar datos a Facebook sin haber obtenido un consentimiento válido de los usuarios.
- A Facebook por tratar esos datos para sus propios fines sin consentimiento.

Y es que, aunque WhatsApp fuese adquirida por Facebook en 2014, y a pesar de que en 2016 se actualizaron los términos de su servicio y política de privacidad incluyendo cambios como el hecho de compartir información de los usuarios de WhatsApp con Facebook, la realidad no era tan bonita. Mientras que los usuarios que ya tenían instalado WhatsApp solo vieron habilitado la opción para rechazar que la información cedida pudiese ser utilizada por Facebook (supuestamente con fines de

[10] https://www.bbc.com/mundo/noticias-43472797

[11] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar

mejora publicitaria), aquellos usuarios nuevos no tenían la posibilidad de rechazar la cesión de información.

La resolución de la AEPD recoge que "exigir que los usuarios presten su consentimiento como requisito para poder hacer uso de la aplicación de mensajería Whatsapp y considerando su implantación social puede entenderse, en los términos del Grupo de Autoridades Europeas de Protección de Datos, como "algo que ejerce una influencia real en la libertad de elección del interesado". El consentimiento, en este caso, no puede considerarse libre y, en consecuencia, no puede considerarse válido."

En este caso, la multa fue de 300.000€, **¿crees que es suficiente o que tiene efecto el poner multas de tal cantidad gigantes empresariales como Facebook? ¿Pondrías otras medidas para asegurarte de que las empresas no usan estas "triquñuelas" para favorecerse?**

3.3. La AEPD vs Google[12]

En 2017, la Agencia Española de Protección de Datos impuso a Google una sanción tras constatar que la compañía había recogido y almacenado datos personales a través de redes WiFi abiertas sin que los usuarios tuviesen conocimiento de dicha recogida.

En este caso, la multa fue de 300.000€, **¿crees que es suficiente o que tiene efecto el poner multas de tal cantidad gigantes tecnológicos como Google? ¿Pondrías otras medidas para asegurarte de que las empresas no usan estas "triquñuelas" para favorecerse?**

3.4. Google+ y sus brechas de seguridad[13]

En 2018, el gigante Google dieron a conocer un error de seguridad que afectó a Google+ en 2015, y es que los datos personales 0.5M de usuarios habían sido expuestos.

En ese mismo año, Google confirmó[14] una nueva brecha de seguridad en la que habían arriesgado la información de 52.5M de usuarios. Datos tan personales como el nombre, el correo electrónico, la ocupación, género o edad habían estado al alcance de cualquier desarrollador por medio de una API.

3.5. Escudo de privacidad Unión Europea – Estados Unidos

El Escudo de Privacidad entre la UE y EEUU nace de la exigencia que impone la Unión Europea para que los datos personales que se han cedido dentro de su marco sigan gozando de un alto nivel de protección al ser transferidos a EEUU.

¿Por qué tendrían que ser transferidos los datos desde la Unión Europea a Estados Unidos? Como resultado de los lazos comerciales entre ambas "entidades", ya que las transferencias de datos personales constituyen una parte importante y necesaria de la relación transatlántica, tal y como proclaman en la guía[15] acerca de este escudo.

---

12 https://www.eleconomista.es/tecnologia/noticias/8727345/11/17/La-AEPD-sanciona-a-Google-con-300000-euros-por-la-recogida-de-datos-sin-consentimiento-a-traves-de-WiFi.html

13 https://www.pandasecurity.com/spain/mediacenter/noticias/google-nueva-brecha-de-seguridad/#:~:text=Se%20trata%20de%20la%20segunda,de%20medio%20mill%C3%B3n%20de%20personas.&text=En%20concreto%2C%20los%20datos%20que,%2C%20ocupaci%C3%B3n%2C%20edad%2C%20etc.

14 https://www.blog.google/technology/safety-security/expediting-changes-google-plus/

15 https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf

Este escudo permite que los datos de una empresa de la Unión Europea se transfieran a otra de Estados Unidos únicamente si dicha empresa procesa los datos personales con arreglo a una serie de protección y salvaguardas ya definidas.

¿Cómo crees que deberían actuar los gobiernos y agencias responsables ante la transmisión ilegal de datos? ¿Regularías la compra venta de datos personales? ¿Harías alguna excepción?