Diputació de València | Protecció de Dades i Seguretat de la Informació

Boletín Protección de Datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 41| Noviembre 2023

MANIPULACIÓN DE LOS USUARIOS EN INTERNET. LOS PATRONES OSCUROS O "DARK PATTERNS"

ÍNDICE

MANIPULACIÓN DE LOS USUARIOS EN INTERNET. LOS PATRONES OSCUROS O "DARK PATTERNS"

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

El término “dark patterns” (patrones oscuros) hace referencia a aquellas estrategias que desarrollan los sitios web o aplicaciones (APPS) con el objetivo de mover al usuario a realizar una acción que, en un principio, éste no tenía pensado hacer. Así, los “dark patterns” se basan en el **engaño, la manipulación o la ocultación de información** para llevar al usuario a realizar algo que no tenía en mente, por ejemplo, comprar un determinado producto, descargar un programa, darse de alta en un servicio, completar un formulario, etc. En resumen, estos patrones consisten en interfaces y la implementación de experiencias en la navegación por la Red, usos de APPS o dispositivos, destinadas a influenciar en el comportamiento de los usuarios, provocando o generando la toma de decisiones no intencionadas o no deseadas.

En aplicación del principio de lealtad establecido en el artículo 5.1.a) del Reglamento General de Protección de Datos (en adelante, RGPD) los responsables del tratamiento han de garantizar que no se emplean patrones oscuros, al menos, con relación a las decisiones respecto del tratamiento de sus datos personales. Estas técnicas están destinadas a influenciar a las personas para que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales.

Recientemente, el Comité Europeo de Protección de Datos (en adelante, EDPB, por sus siglas en inglés) adoptó para consulta pública sus *‘Directrices sobre “dark patterns” en interfaces de redes sociales: Cómo reconocerlos y evitarlos’.* Estas directrices, toman como punto de partida el artículo 5.1.a) del RGPD, recogen una serie de ejemplos, así como recomendaciones de buenas prácticas para evitar los “dark patterns”.

"DARK PATTERNS" Y SUS CATEGORIAS

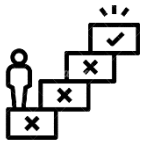
Los "dark patterns" pueden presentarse al usuario en operaciones de tratamiento de diversa índole, como durante el proceso de registro o alta en una red social, al iniciar sesión o también en otros escenarios como en la configuración de las opciones de privacidad, en los banners de cookies, durante el proceso de ejercicio de derechos, en el contenido de una comunicación informando sobre una brecha de datos personales o incluso al intentar darse de baja de la plataforma.
De acuerdo con las Directrices del EDPB, los "dark patterns" pueden clasificarse en las siguientes categorías:

- **Sobrecarga (overloading):** consiste en presentar demasiadas posibilidades a la persona que tiene que tomar las decisiones, lo que termina generando fatiga sobre el usuario, que acaba compartiendo más información personal de la deseada. Las técnicas más habituales para producir esa fatiga por sobrecarga son mostrar preguntas de forma reiterada, crear laberintos de privacidad y mostrar demasiadas opciones.

- **Ocultación (skipping):** consiste en diseñar la interfaz o experiencia de usuario de tal manera que el usuario no piense en algunos aspectos relacionados con la protección de sus datos, o que lo olvide. Forman parte de esta categoría los dos patrones oscuros siguientes: comodidad engañosa y mirar hacia allí.

- **Emocionar (stirring):** se apela a las emociones de los usuarios o se utilizan empujones visuales en forma de efectos para influenciar en las decisiones. Los siguientes dos patrones oscuros forman parte de esta categoría: dirección emocional y oculto a plena vista.

- **Obstaculización (hindering):** trata de poner trabas para que el usuario no pueda realizar de forma sencilla ciertas acciones. Esto se realiza a través de técnicas como poner los ajustes de privacidad en zonas a las que no se puede acceder, que sea muy complicado llegar hasta ellas o proporcionando información engañosa sobre los efectos de algunas acciones. Los siguientes tres patrones oscuros forman parte de esta categoría: callejón sin salida, más tiempo del necesario e información engañosa.



- **Inconsistencia (fickle):** la interfaz presenta un diseño inestable e inconsistente que no permite realizar las acciones deseadas por el usuario. Como resultado, al usuario le resulta difícil navegar entre las distintas herramientas de control de la protección de datos y comprender la finalidad del tratamiento. Los dos siguientes patrones oscuros forman parte de esta categoría: falta de jerarquía y descontextualización.

- **Enturbiar (left in the dark):** la información o las opciones de configuración de la privacidad se esconden o se presentan de forma poco clara utilizando un lenguaje errático, información contradictoria o ambigua para dejar a los usuarios sin saber cómo se tratan sus datos y cómo pueden

controlarlos ejerciendo sus derechos. Los siguientes tres patrones oscuros forman parte de esta categoría: discontinuidad lingüística, información contradictoria y redacción o información ambigua.

PRINCIPIOS DE PROTECCION DE DATOS

Otros principios de protección de datos que juegan un papel clave en la evaluación de los *"dark patterns"* son los **de transparencia, minimización de datos y responsabilidad proactiva**, en cuanto a privacidad por defecto. También, en ciertas ocasiones, el principio de limitación de la finalidad, las condiciones de obtención del consentimiento y la transparencia en la información proporcionada para el ejercicio de derechos.

En todo caso, el **principio de protección de datos desde el diseño y por defecto debe aplicarse desde el momento de concepción de las interfaces y experiencias de usuarios**, antes del lanzamiento; para garantizar los derechos y libertades fundamentales de las personas, así como el cumplimiento de la normativa.

Para cumplir con los principios de transparencia y equidad, es necesario garantizar que los usuarios puedan disponer de toda la información necesaria sobre la forma en que se tratan sus datos; para que puedan tomar las decisiones que les corresponden o ejercer sus derechos, y que el tratamiento sea conforme a las expectativas que el interesado haya podido generar a partir de dicha información.

Por supuesto, el responsable del tratamiento de los datos de carácter personal debe determinar el contenido de las cláusulas de información. A continuación, se indican aspectos importantes que deben tenerse en cuenta a este respecto.

¿QUÉ ASPECTOS IMPORTANTES HAY QUE TENER EN CUENTA?

- La **información debe facilitarse antes de recabar los datos** y, en su caso, antes de dar el consentimiento.

- **Cuando los datos no se obtienen de la persona afectada, también es necesario informarle**. Esto debe hacerse en el plazo de un mes desde la obtención de los datos o, si se prevé que los datos se utilizarán en comunicaciones, a más tardar cuando se realice la primera comunicación al afectado o a un tercero.

- La información debe ser **completa, sencilla, comprensible**, visualmente clara y, en su caso, adaptada a personas con dificultades funcionales.

- En el caso de los servicios dirigidos a los **menores, la información debe facilitarse en un lenguaje adaptado al nivel de conocimientos** de este colectivo. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender (Considerando 58 RGDP).

- La información puede proporcionarse por **capas.** Así, inicialmente se facilita información sobre la finalidad del tratamiento, la identidad del responsable del tratamiento y la posibilidad de ejercer los derechos de autodeterminación informativa (acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad), así como cualquier otra información que se considere imprescindible.

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/proteccciondatos

- La información facilitada debe ser exacta. Los usuarios deben ser informados. Los usuarios deben ser informados clara y rápidamente de cualquier cambio para que puedan tomar las decisiones adecuadas. tomar las decisiones adecuadas.

- Es necesario permitir la realización de copias de los sitios web y aplicaciones, para poder verificar los mecanismos y el contenido de las cláusulas informativas existentes en cada momento mediante la aplicación de un sello de tiempo verificable.

- Es necesario abstenerse de implementar patrones oscuros.

LEGITIMACIÓN DE LOS TRATAMIENTOS

Los responsables del tratamiento deben seleccionar las opciones de configuración adecuadas de forma que se asegure que sólo se recopilarán los datos estrictamente necesarios para alcanzar el propósito del tratamiento que se ha habilitado.

Hay que tener presente que, este caso de mínima intrusión puede no ser único y que, en función de la complejidad del tratamiento, podrían existir varios casos de uso restrictivos. En esa circunstancia, el responsable deberá justificar la elección de aquel que se haya establecido por defecto.

El usuario tendrá que modificar la configuración por defecto si quiere ampliar el tratamiento de datos personales más allá de la base legal en la que se basa el tratamiento principal para el que se ha realizado la configuración “por defecto” o si las nuevas funcionalidades implican propósitos no compatibles con el propósito original para el que inicialmente se recopilaron los datos personales.

En aplicación del principio de lealtad establecido en el artículo 5.1.a) del RGPD, el responsable del tratamiento ha de garantizar que no se emplean los “dark patterns”, mediante interfaces de usuario diseñadas para influir, a través de manipulaciones psicológicas y de forma encubierta, en las elecciones del interesado, al menos, con relación al tratamiento de sus datos personales.

LOS "DARK PATTERNS" ANTE LA JUSTICIA

Los "dark pattners" pueden favorecer que se violen las regulaciones tanto RGPD, como de la Ley de Servicios Digitales (en adelante, DSA), así como otras legislaciones vigentes.

Las sanciones por incumplimiento pueden variar según la gravedad de la infracción. Conforme al artículo 83 del RGPD, las multas pueden ascender hasta **20 millones de euros o el 4% del volumen de negocio total anual global** del ejercicio financiero anterior, aplicándose la cuantía mayor en caso de infracciones muy graves.

La recién estrenada Ley de Servicios Digitales, que entró en vigor el 25 de agosto de 2023 también cuenta con severas sanciones. Esta ley establece obligaciones en relación a la transparencia y consentimiento, la desinformación y las obligaciones para establecer un entorno digital seguro. Aplica proporcionalmente a todos los servicios digitales que conecten bienes, servicios o contenidos con consumidores. Las multas pueden alcanzar hasta el **6% de la facturación global de la empresa.**

A esto hay que añadir vulneraciones que también se puedan llevar a cabo con leyes nacionales. En el caso de España la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) que contempla sanciones relacionadas con las cookies.

En este contexto, la Agencia Española de Protección de Datos (en adelante, AEPD**)** emitió el pasado mes de septiembre un procedimiento contra la empresa Chatwith.io Worldwide S.L. Se trata de la primera multa por uso de "*dark patterns*", con una sanción de **12.000 euros** por diversas infracciones:

- **Deficiencias en el tratamiento de datos personales** de la web y la Política de Privacidad: por incumplimiento del principio de transparencia o el derecho de información del afectado por no facilitar toda la información exigida; infracción al art. 13 del RGPD
- **Uso de patrones oscuros de sobrecarga (overloading) y ocultación (skipping)** en la configuración de opciones de privacidad, y "cuando el interesado manifiesta su oposición al tratamiento de datos basado en el interés legítimo del responsable y de terceros, a los que este denomina socios", lo cual infringe el principio de transparencia del art. 5.1.a) del RGPD por el que: "Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado «licitud, lealtad y transparencia»".
- **Deficiencias en la Política de Cookies** de la web, por la instalación de cookies sin consentimiento previo y la falta de información clara al usuario, infringiendo el art. 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

MATERIAL COMPLEMENTARIO

- Guía sobre la aplicación de la protección de datos por defecto, o PDpD. Puedes consultar la guía en este enlace.
- Directrices 3/2022 sobre Patrones oscuros en las interfaces de plataformas de redes sociales del EDPB: cómo reconocerlos y evitarlos. Puedes consultar estas Directrices en este enlace.
- Resolución de la AEPD PS/00080/2023 sobre la reclamación dirigida contra CHATWITH.IO. WORLDWIDE, S.L. Puedes consultar la Resolución en este enlace.
- Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, sobre un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de servicios digitales DSA). Puedes consultar la norma en este enlace.

NOTICIAS

- **La AEPD sanciona al Ayuntamiento de Migjorn Gran por una infracción del artículo 32.1 del RGPD al remitir una notificación en la que en el exterior del sobre utilizado figuraba el nº de DNI completo del reclamante junto a su nombre, apellidos y dirección**

  El reclamado remitió una notificación y en el exterior del sobre utilizado figuraba el nº de DNI completo del reclamante junto a su nombre, apellidos y dirección, posibilitando que un tercero que haya visto el sobre o participado en el proceso postal desde que salió del reclamado hasta que fue entregado en mano en su domicilio pudiera tomar nota de ello. En la resolución la AEPD indica que el reclamado vulneró la normativa en materia de protección de datos de carácter personal al infringirse las medidas técnicas y organizativas implantadas.

  Puedes consultar la Resolución en este enlace.

- **El Tribunal Superior de Justicia de Cataluña manifiesta que el derecho de desconexión digital no es un derecho fundamental**

  Los incumplimientos en los que incurrió la empresa comportaron que el trabajador se viera expuesto a jornadas muy prolongadas y en horarios intempestivos, pudieron comprometer su derecho al descanso y a la desconexión digital, lo que ha podido incidir en el proceso de incapacidad temporal en el que se encuentra, pero tales incumplimientos, si bien generan derecho a extinguir voluntariamente el contrato de trabajo con la indemnización correspondiente, no generan una indemnización adicional de daños y perjuicios porque no se han vulnerado derechos fundamentales. El derecho al descanso y a la limitación del tiempo de trabajo aparecen en el artículo 40.2 CE dentro de los principios rectores de la política social y económica, pero no dentro del capítulo dedicado a los derechos fundamentales.

  Puedes consultar la Sentencia en este enlace.