DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 29 | Noviembre 2022

DARK PATTERNS (PATRONES OSCUROS): BUENAS PRÁCTICAS

Í N D I C E

DARK PATTERNS (PATRONES OSCUROS)

	Página
Introducción: ¿Qué son los *dark patterns?*	**2**
Categorías	**3**
Buenas prácticas	**4**
Material complementario y noticias	**8**

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 suscribirte a nuestra publicación accede al siguiente

enlace

INTRODUCCIÓN: ¿QUÉ SON LOS *DARK PATTERNS*?

El término *dark patterns* (patrones oscuros) hace referencia interfaces e implementaciones de experiencia de usuario destinadas a influenciar en el comportamiento y las decisiones de las personas en su interacción con webs, *apps* y redes sociales, de forma que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales. Esto es, se trata de prácticas poco respetuosas que buscan manipular la interacción de las personas, como: presentar demasiadas posibilidades a los usuarios que tienen que tomar las decisiones para fatigarles, apelar a sus emociones para influenciar en sus decisiones, ponerles trabas para que no puedan realizar de forma sencilla ciertas acciones, etc.

Los *dark patterns* pueden presentarse al usuario en operaciones de tratamiento de diversa índole, como durante el proceso de registro o alta en una web, *app* o 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.

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 *dark patterns*, al menos, en relación con el tratamiento de sus datos personales. 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. En algunas ocasiones también 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

"EL TÉRMINO DARK PATTERNS (PATRONES OSCUROS) HACE REFERENCIA INTERFACES E IMPLEMENTACIONES DE EXPERIENCIA DE USUARIO DESTINADAS A INFLUENCIAR EN EL COMPORTAMIENTO Y LAS DECISIONES DE LAS PERSONAS EN SU INTERACCIÓN CON WEBS, APPS Y REDES SOCIALES, DE FORMA QUE TOMEN DECISIONES POTENCIALMENTE PERJUDICIALES PARA LA PROTECCIÓN DE SUS DATOS PERSONALES".

lanzamiento, para garantizar los derechos y libertades fundamentales de las personas, así como el cumplimiento de la normativa.

El presente Cuaderno, teniendo en cuenta las recomendaciones de la Agencia Española de Protección de Datos (AEPD) y del Comité Europeo de Protección de Datos (CEPD), trata de establecer una relación de elementos a tener en cuenta para que en la creación y configuración de las webs, *apps* o redes sociales de la Diputación no se empleen *dark patterns* para manipular el proceso de elección del usuario o influir de forma encubierta en su decisión respecto al alcance del tratamiento.

"SE DEBE ESTABLECER UNA RELACIÓN DE ELEMENTOS A TENER EN CUENTA PARA QUE EN LA CREACIÓN Y CONFIGURACIÓN DE LAS WEBS, APPS O REDES SOCIALES DE LA DIPUTACIÓN NO SE EMPLEEN DARK PATTERNS PARA MANIPULAR EL PROCESO DE ELECCIÓN DEL USUARIO O INFLUIR DE FORMA ENCUBIERTA EN SU DECISIÓN RESPECTO AL ALCANCE DEL TRATAMIENTO".

CATEGORÍAS

El CEPD, en su documento de 'Directrices 3/2022 sobre patrones oscuros en las interfaces de las plataformas de redes sociales: cómo reconocerlos y evitarlos' (versión 1.0, del 14 de marzo de 2022), divide los *dark patterns* en las siguientes categorías:

- **SOBRECARGA:** los usuarios se enfrentan a una avalancha/gran cantidad de solicitudes, información, opciones o posibilidades para pedirles que compartan más datos o permitir involuntariamente el tratamiento de datos personales en contra de las expectativas del interesado.

- **OMISIÓN**: diseñar la interfaz o la experiencia del usuario de una manera que los usuarios olviden o no piensen en todos o algunos de los aspectos de protección de datos.

- **EMOCIÓN:** afecta la elección que harían los usuarios apelando a sus emociones.

- **OBSTACULIZACIÓN*:*** entorpecer o bloquear a los usuarios en su proceso de informarse o administrar sus datos haciendo que la acción sea difícil o imposible de lograr.

"INFLUIR EN LAS DECISIONES AL PROPORCIONAR INFORMACIÓN SESGADA A LAS PERSONAS PUEDE CONSIDERARSE UNA PRÁCTICA DESLEAL".

- **INCONSISTENCIA:** el diseño de la interfaz es inconsistente y poco claro, lo que dificulta que el usuario navegue por las diferentes herramientas de control de protección de datos y comprenda el propósito del tratamiento.

- **ENTURBIAR:** cuando una interfaz está diseñada para ocultar información o herramientas de control de protección de datos o dejar a los usuarios inseguros sobre cómo se tratan sus datos y qué tipo de control pueden tener sobre ellos con respecto al ejercicio de sus derechos.

BUENAS PRÁCTICAS

- No se debe solicitar a los usuarios más datos personales de los necesarios para los fines del tratamiento.

- En caso de solicitar datos opcionales, no se debe hacer de manera continua. Si los usuarios se han negado previamente a facilitar un dato y la solicitud se repite, esta solicitud continua puede influir en los usuarios para que simplemente acepten la solicitud de la plataforma para finalmente completar el proceso.

- Además, el lenguaje utilizado no debería transmitir una sensación de urgencia o sonar como un imperativo. Si los usuarios sienten esta obligación, aun cuando en realidad no sea obligatorio facilitar los datos, esto puede tener un impacto en su "libre albedrío".

- No se deben utilizar palabras o imágenes de una manera que transmitan información a los usuarios en una perspectiva muy positiva, haciendo que los usuarios se sientan bien o seguros, o muy negativa, haciendo que los usuarios se sientan ansiosos o culpables.

"LOS INTERESADOS DEBEN RECIBIR INFORMACIÓN DE MANERA CLARA PARA QUE PUEDAN COMPRENDER CÓMO SE TRATAN SUS DATOS PERSONALES Y CÓMO PUEDEN CONTROLARLOS. ADEMÁS, ESTA INFORMACIÓN TIENE QUE SER ACCESIBLE Y FÁCILMENTE PERCEPTIBLE POR LOS INTERESADOS".

- El proceso de registro o ingreso de datos no debe llevar más tiempo del necesario. Cuando los usuarios intentan activar un control relacionado con la protección de datos, pero la experiencia del usuario se hace de tal manera que requiere que los usuarios completen más pasos en comparación con la cantidad de pasos necesarios para la activación de las opciones invasivas de datos, es probable que esto disuada a los usuarios de activar los controles de protección de datos.

- Cuando a los usuarios se les proporciona una opción relacionada con la protección de datos durante el proceso de registro, estos deben poder encontrar esa opción más tarde, mientras hacen uso del servicio.

- Se debe tener en cuenta el principio de protección de datos por defecto. Cuando la configuración de datos está preseleccionada, los usuarios están sujetos a un nivel de protección de datos específico, determinado por el responsable del tratamiento de forma predeterminada, en lugar de por los usuarios. Debido al efecto que empuja a las personas a mantener una opción preseleccionada, es poco probable que los usuarios las cambien, incluso si se les da la posibilidad. Por eso, en caso de que una de las opciones estuviera preseleccionada, esta debería ser, por defecto, la opción más respetuosa con la privacidad de los usuarios.

- De conformidad con el principio de transparencia, los interesados deben recibir información de manera clara para que puedan comprender cómo se tratan sus datos personales y cómo pueden controlarlos. Además, esta información tiene que ser accesible y fácilmente perceptible por los interesados.

- Proporcionar la información en capas puede ayudar a presentar el aviso de privacidad con mayor claridad. Sin embargo, esto no debería dificultar innecesariamente el ejercicio de funciones o derechos de los usuarios. Estos no deberían tener que navegar a través de diferentes páginas sin tener disponible una visión completa y exhaustiva.

"LA REDACCIÓN QUE SE DA A LA INFORMACIÓN NO DEBE SER AMBIGUA O IMPRECISA. DE LO CONTRARIO, ES PROBABLE QUE LOS USUARIOS NO ESTÉN SEGUROS DEL TRATAMIENTO QUE SE DARÁ A SUS DATOS. POR EJEMPLO, SE DEBEN EVITAR EXPRESIONES COMO: SUS DATOS PODRÍAN USARSE PARA MEJORAR NUESTROS SERVICIOS".

- Cuando los servicios están dirigidos a niños, debemos asegurarnos de que el lenguaje utilizado, incluido su tono y estilo, sea apropiado para que comprendan fácilmente la información proporcionada.

- El uso de un tamaño de fuente pequeño o el uso de colores que no contrasten lo suficiente como para ofrecer una legibilidad suficiente (por ejemplo, un color de texto gris tenue sobre un fondo blanco) puede tener un impacto negativo en los usuarios, ya que el texto será menos visible y los usuarios lo pasarán por alto o tendrán dificultades para leerlo. Especialmente, se da este caso cuando se colocan uno o más elementos llamativos junto a la información obligatoria relacionada con la protección de datos. Estas técnicas de interfaz deben evitarse, ya que engañan a los usuarios y hacen que la identificación de la información relacionada con la protección de sus datos sea más lenta, ya que requiere más tiempo y atención para detectar la información relevante.

- La presentación de la información debe seguir un orden o una jerarquía. La información relativa a la protección de datos que carece de jerarquía se da cuando dicha información aparece varias veces y se presenta de formas diferentes. Es probable que los usuarios se sientan confundidos por esta redundancia y no puedan comprender completamente cómo se tratan sus datos y cómo ejercer control sobre ellos.

  La falta de jerarquía también puede surgir cuando la información dada está estructurada de una manera que dificulta la orientación de los usuarios, por ejemplo, cuando la Política de Privacidad cuenta con más de 70 páginas y no se proporciona un menú de navegación o índice que permita a los usuarios acceder fácilmente a la sección que buscan.

- La redacción que se da a la información no debe ser ambigua o imprecisa. De lo contrario, es probable que los usuarios no estén seguros del tratamiento que se dará a sus datos. Por ejemplo, se deben evitar expresiones como *"Sus datos podrían usarse para mejorar nuestros servicios".* En este caso, el uso del tiempo condicional *"podría"* deja a los usuarios sin

saber si sus datos se utilizarán o no y es probable que el término *"servicios"* sea demasiado general para calificarlo como claro.

- En numerosas ocasiones, en la interfaz se utiliza un interruptor para permitir que los usuarios proporcionen o retiren su consentimiento para determinadas finalidades. Sin embargo, hay veces que la forma en la que están diseñados esos interruptores no dejan claro en qué posición se encuentra.

La información visual no debe dar lugar a equívoco. Esto es, debe quedar claro para el usuario cuándo el interruptor está en modo "consentimiento" y cuándo no.

"CUANDO EN LA INTERFAZ SE UTILIZA UN INTERRUPTOR PARA PERMITIR QUE LOS USUARIOS PROPORCIONEN O RETIREN SU CONSENTIMIENTO PARA DETERMINADAS FINALDIADES, HEMOS DE CERCIORARNOS DE QUE LA INFORMACIÓN VISUAL NO DÉ LUGAR A EQUÍVOCO. ESTO ES, DEBE QUEDAR CLARO PARA EL USUARIO CUÁNDO EL INTERRUPTOR ESTÁ EN MODO CONSENTIMIENTO Y CUÁNDO NO".

MATERIAL COMPLEMENTARIO

- Directrices 3/2022 sobre patrones oscuros en las interfaces de las plataformas de redes sociales: cómo reconocerlos y evitarlos (CEPD).

  Consulta este enlace.

- *Dark patterns:* Manipulación en los servicios de Internet (Blog AEPD).

  Consulta este enlace.

- Guía de Protección de Datos por Defecto (AEPD).

  Consulta este enlace.

- *DARK PATTERNS* I: Los *dark patterns* como amenaza a la privacidad de los usuarios (Blog Asociación Española para la Calidad).

  Consulta este enlace.

- Los reyes de los *dark patterns* en términos de privacidad: los banners de las cookies (Blog Asociación Española para la Calidad).

  Consulta este enlace.

NOTICIAS

- **La AEPD estrena en su web una sección sobre el tratamiento de datos en Administraciones Públicas.**

  La sección dedicada a los tratamientos llevados a cabo por las Administraciones Públicas tiene como objetivo agrupar todos aquellos recursos que se encuentran disponibles en la web de la AEPD para que puedan ser utilizados por los responsables, y especialmente, por las personas que tienen asignada la función de delegado de protección datos y sus equipos, facilitando así el ejercicio de su labor. Consulta la nueva sección en este enlace.

- **La AEPD lanza una herramienta para ayudar a los responsables a decidir si deben notificar una brecha de datos a la autoridad de control.**

  La Agencia Española de Protección de Datos (AEPD) ha lanzado la herramienta 'Asesora Brecha', que tiene como objetivo ayudar a los responsables de tratamientos a decidir si deben notificar una brecha de datos personales a la autoridad de control. Esta herramienta también puede ser utilizada por delegados de protección de datos, encargados de tratamiento o consultores para obtener información adecuada con la que asesorar a los responsables. Consulta la noticia en este enlace.

- **La AEPD sanciona al Servicio de Salud de Castilla La Mancha por enviar un email a varios de sus trabajadores con datos (incluidos datos de salud) de otros.**

  La AEPD sanciona al Servicio de Salud de Castilla La Mancha por enviar un email a varios de sus trabajadores con sus nombres, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad y si esto había conllevado una baja laboral. El email no contenía únicamente la información relativa a cada destinatario sino también la de todos los demás. Consulta la Resolución en este enlace.