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

# Butlletí Protecció de Dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 41| Novembre 2023

## MANIPULACIÓ DELS USUARIS EN INTERNET. ELS PATRONS FOSCOS O "DARK PATTERNS"

# ÍNDEX

## MANIPULACIÓ DELS USUARIS EN INTERNET. ELS PATRONS FOSCOS O "DARK PATTERNS"

**INTRODUCCIÓ.....2**
**"DARK PATTERNS" I ELS SEUS CATEGORIAS .....3**
**PRINCIPIS DE PROTECCION DE DADES .....4**
**QUINS ASPECTES IMPORTANTS CAL TINDRE EN COMPTE? .....4**
**LEGITIMACIÓ DELS TRACTAMENTS.....5**
**ELS ""DARK PATTERNS"" DAVANT LA JUSTÍCIA .....6**
**NOTÍCIES.....7**

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Estes peticions hauran de dirigir-se a:

Diputació de València

Dpto. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

## INTRODUCCIÓ

El terme "*dark patterns*" (patrons foscos) fa referència a aquelles estratègies que desenvolupen els llocs web o aplicacions (APPS) amb l'objectiu de moure a l'usuari a realitzar una acció que, en un principi, este no tenia pensat fer. Així, els "*dark patterns*" es basen en l'engany, **la manipulació o l'ocultació d'informació** per a portar a l'usuari a realitzar alguna cosa que no tenia al cap, per exemple, comprar un determinat producte, descarregar un programa, donar-se d'alta en un servei, completar un formulari, etc. En resum, estos patrons consisteixen en interfícies i la implementació d'experiències en la navegació per la Xarxa, usos d'APPS o dispositius, destinades a influenciar en el comportament dels usuaris, provocant o generant la presa de decisions no intencionades o no desitjades.

En aplicació del principi de lleialtat establit en l'article 5.1.a) del Reglament General de Protecció de Dades (d'ara en avant, RGPD) els responsables del tractament han de garantir que no s'empren patrons foscos, almenys, en relació amb les decisions respecte del tractament de les seues dades personals. Estes tècniques estan destinades a influenciar a les persones perquè prenguen decisions potencialment perjudicials per a la protecció de les seues dades personals.

Recentment, el Comité Europeu de Protecció de Dades (d'ara en avant, EDPB, per les seues sigles en anglès) va adoptar per a consulta pública les seues *'Directrius sobre "dark patterns" en interfícies de xarxes socials: Com reconèixer-los i evitar-los'.* Estes directrius, prenen com a punt de partida l'article 5.1.a) del RGPD, i recullen una sèrie d'exemples, així com recomanacions de bones pràctiques per a evitar els "*dark patterns*".

## "DARK PATTERNS" I ELS SEUS CATEGORIAS

Els "*dark patterns*" poden presentar-se a l'usuari en operacions de tractament de diversa índole, com durant el procés de registre o alta en una xarxa social, en iniciar sessió o també en altres escenaris com en la configuració de les opcions de privacitat, en els bàners de cookies, durant el procés d'exercici de drets, en el contingut d'una comunicació informant sobre una bretxa de dades personals o fins i tot en intentar donar-se de baixa de la plataforma.

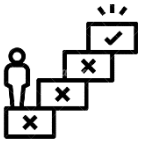
D'acord amb les Directrius del EDPB, els "*dark patterns*" poden classificar-se en les següents categories:

- **Sobrecàrrega (*overloading*):** consisteix a presentar massa possibilitats a la persona que ha de prendre les decisions, la qual cosa acaba generant fatiga sobre l'usuari, que acaba compartint més informació personal de la desitjada. Les tècniques més habituals per a produir eixa fatiga per sobrecàrrega són mostrar preguntes de manera reiterada, crear laberints de privacitat i mostrar massa opcions.

- **Ocultació (*skipping*):** consisteix a dissenyar la interfície o experiència d'usuari de tal manera que l'usuari no pense en alguns aspectes relacionats amb la protecció de les seues dades, o que l'oblide. Formen part d'esta categoria els dos patrons foscos següents: comoditat enganyosa i mirar cap a allí.

- **Emocionar (*stirring*):** s'apel·la a les emocions dels usuaris o s'utilitzen espentes visuals en forma d'efectes per a influenciar en les decisions. Els següents dos patrons foscos formen part d'esta categoria: direcció emocional i ocult a plena vista.

- **Obstaculització (*hindering*):** tracta de posar traves perquè l'usuari no puga realitzar de manera senzilla unes certes accions. Això es realitza a través de tècniques com posar els ajustos de privacitat en zones a les quals no es pot accedir, que siga molt complicat arribar fins elles o proporcionant informació enganyosa sobre els efectes d'algunes accions. Els següents tres patrons foscos formen part d'esta categoria: atzucac, més temps del necessari i informació enganyosa.



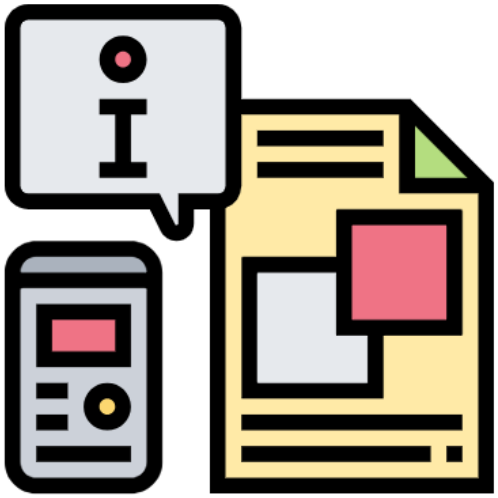
- **Inconsistència (*fickle*):** la interfície presenta un disseny inestable i inconsistent que no permet realitzar les accions desitjades per l'usuari. Com a resultat, a l'usuari li resulta difícil navegar entre les diferents eines de control de la protecció de dades i comprendre la finalitat del tractament. Els dos següents patrons foscos formen part d'esta categoria: falta de jerarquia i descontextualització.

- **Enterbolir (*left in the dark*):** la informació o les opcions de configuració de la privacitat s'amaguen o es presenten de forma poc clara utilitzant un llenguatge erràtic, informació contradictòria o ambigua

per a deixar als usuaris sense saber com es tracten les seues dades i com poden controlar-los exercint els seus drets. Els següents tres patrons foscos formen part d'esta categoria: discontinuïtat lingüística, informació contradictòria i redacció o informació ambigua.

## PRINCIPIS DE PROTECCION DE DADES

Altres principis de protecció de dades que juguen un paper clau en l'avaluació dels *"dark patterns"* són els **de transparència, minimització de dades i responsabilitat proactiva,** quant a privacitat per defecte. També, en unes certes ocasions, el principi de limitació de la finalitat, les condicions d'obtenció del consentiment i la transparència en la informació proporcionada per a l'exercici de drets.



En tot cas, el **principi de protecció de dades des del disseny i per defecte ha d'aplicar-se des del moment de concepció de les interfícies i experiències d'usuaris**, abans del llançament; per a garantir els drets i llibertats fonamentals de les persones, així com el compliment de la normativa.

Per a complir amb els principis de transparència i equitat, és necessari garantir que els usuaris puguen disposar de tota la informació necessària sobre la forma en què es tracten les seues dades; perquè puguen prendre les decisions que els corresponen o exercir els seus drets, i que el tractament siga conforme a les expectatives que l'interessat haja pogut generar a partir d'aquesta informació.

Per descomptat, el responsable del tractament de les dades de caràcter personal ha de determinar el contingut de les clàusules d'informació. A continuació, s'indiquen aspectes importants que han de tindre's en compte referent a això.

## QUINS ASPECTES IMPORTANTS CAL TINDRE EN COMPTE?

- La **informació ha de facilitar-se abans de recaptar les dades** i, si és el cas, abans de donar el consentiment.

- **Quan les dades no s'obtenen de la persona afectada, també és necessari informar-lo**. Això ha de fer-se en el termini d'un mes des de l'obtenció de les dades o, si es preveu que les dades s'utilitzaran en comunicacions, a tot tardar quan es realitze la primera comunicació a l'afectat o a un tercer.

- La informació ha de ser **completa, senzilla, comprensible**, visualment clara i, si és el cas, adaptada a persones amb dificultats funcionals.

- En el cas dels serveis dirigits a l'ús per part de **menors, la informació ha de facilitar-se en un llenguatge adaptat al nivell de coneixements** d'este col·lectiu. Atés que els xiquets mereixen una protecció específica, qualsevol informació i comunicació el tractament de la qual els afecte ha de facilitar-se en un llenguatge clar i senzill que siga fàcil d'entendre (Considerant 58 RGDP).

- La informació pot proporcionar-se per **capes.** Així, inicialment es facilita informació sobre la finalitat del tractament, la identitat del responsable del tractament i la possibilitat d'exercir els drets d'autodeterminació informativa (accés, rectificació, supressió, oposició, limitació del tractament i portabilitat), així com qualsevol altra informació que es 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/protecciondatos |

- La informació facilitada ha de ser exacta. Els usuaris han de ser informats. Els usuaris han de ser informats clara i ràpidament de qualsevol canvi perquè puguen prendre les decisions adequades.

- És necessari permetre la realització de còpies dels llocs web i aplicacions, per a poder verificar els mecanismes i el contingut de les clàusules informatives existents a cada moment mitjançant l'aplicació d'un segell de temps verificable.

- És necessari abstindre's d'implementar patrons foscos.

## LEGITIMACION DELS TRACTAMENTS

Els responsables del tractament han de seleccionar les opcions de configuració adequades de manera que s'assegure que només es recopilaran les dades estrictament necessàries per a aconseguir el propòsit del tractament que s'ha habilitat.

Cal tindre present que, este cas de mínima intrusió pot no ser únic i que, en funció de la complexitat del tractament, podrien existir diversos casos d'ús restrictius. En eixa circumstància, el responsable haurà de justificar l'elecció d'aquell que s'haja establit per defecte.

L'usuari haurà de modificar la configuració per defecte si vol ampliar el tractament de dades personals més enllà de la base legal en la qual es basa el tractament principal per al qual s'ha realitzat la configuració "*per defecte*" o si les noves funcionalitats impliquen propòsits no compatibles amb el propòsit original per al qual inicialment es van recopilar les dades personals.

En aplicació del principi de lleialtat establit en l'article 5.1.a) del RGPD, el responsable del tractament ha de garantir que no s'empren els "*dark patterns*", mitjançant interfícies d'usuari dissenyades per a influir, a través de manipulacions psicològiques i de forma encoberta, en les eleccions de l'interessat, almenys, en relació amb el tractament de les seues dades personals.

## ELS "*DARK PATTERNS*" DAVANT LA JUSTÍCIA

Els "*dark pattners*" poden afavorir que es violen les regulacions tant de RGPD, com de la Llei de Serveis Digitals (d'ara en avant, DSA), així com altres legislacions vigents.

Les sancions per incompliment poden variar segons la gravetat de la infracció. Conforme a l'article 83 del RGPD, les multes poden ascendir fins a **20 milions d'euros o el 4% del volum de negoci total anual global** de l'exercici financer anterior, aplicant-se la quantia major en cas d'infraccions molt greus.

La recentment estrenada Llei de Serveis Digitals, que va entrar en vigor el 25 d'agost de 2023 també compta amb severes sancions. Esta llei estableix obligacions en relació a la transparència i consentiment, la desinformació i les obligacions per a establir un entorn digital segur. Aplica proporcionalment a tots els serveis digitals que connecten béns, serveis o continguts amb consumidors. Les multes poden aconseguir fins al 6% **de la facturació global de l'empresa.**

A això cal afegir vulneracions que també es puguen dur a terme amb lleis nacionals. En el cas d'Espanya la Llei de Serveis de la Societat de la Informació de Comerç Electrònic (LSSI) que contempla sancions relacionades amb les cookies.

En este context, l'Agència Espanyola de Protecció de Dades (d'ara en avant, AEPD) va emetre el mes de setembre passat un procediment contra l'empresa Chatwith.io Worldwide S.L. Es tracta de la primera multa per ús de "*dark patterns*", amb una sanció de **12.000 euros** per diverses infraccions:

- **Deficiències en el tractament de dades personals** de la web i la Política de Privacitat: per incompliment del principi de transparència o el dret d'informació de l'afectat per no facilitar tota la informació exigida; infracció al art. 13 del RGPD.

- **Ús de patrons foscos de sobrecàrrega (*overloading*) i ocultació (*skipping*)** en la configuració d'opcions de privacitat, i "*quan l'interessat manifesta la seua oposició al tractament de dades basat en l'interés legítim del responsable i de tercers, als quals este denomina socis*", la qual cosa infringeix el principi de transparència del art. 5.1.a) del RGPD pel qual: "*Les dades personals seran tractats de manera lícita, lleial i transparent en relació amb l'interessat «licitud, lleialtat i transparència»*".

- **Deficiències en la Política de Cookies** de la web, per la instal·lació de cookies sense consentiment previ i la falta d'informació clara a l'usuari, infringint el art. 22.2 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI).

## MATERIAL COMPLEMENTARI

- Guia sobre l'aplicació de la protecció de dades per defecte, o PDPD. Pots consultar la guia en este enllaç.
- Directrius 3/2022 sobre Patrons foscos en les interfícies de plataformes de xarxes socials del EDPB: com reconèixer-los i evitar-los. Pots consultar estes Directrius en este enllaç.
- Resolució de l'AEPD PS/00080/2023 sobre la reclamació dirigida contra CHATWITH.IO. WORLDWIDE, S.L. Pots consultar la Resolució en este enllaç.
- Reglament (UE) 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, sobre un mercat únic de serveis digitals i pel qual es modifica la Directiva 2000/31/CE (Llei de serveis digitals DSA). Pots consultar la norma en este enllaç.

# NOTÍCIES

- **L'AEPD sanciona a l'Ajuntament de Migjorn Gran per una infracció de l'article 32.1 del RGPD en remetre una notificació en la qual en l'exterior del sobre utilitzat figurava el núm. de DNI complet del reclamant al costat del seu nom, cognoms i adreça**

  El reclamat va remetre una notificació i en l'exterior del sobre utilitzat figurava el núm. de DNI complet del reclamant al costat del seu nom, cognoms i adreça, possibilitant que un tercer que haja vist el sobre o participat en el procés postal des que va eixir del reclamat fins que va ser entregat en mà en el seu domicili poguera prendre nota d'això. En la resolució l'AEPD indica que el reclamat va vulnerar la normativa en matèria de protecció de dades de caràcter personal en infringir-se les mesures tècniques i organitzatives implantades.

  Pots consultar la Resolució en este enllaç.

- **El Tribunal Superior de Justícia de Catalunya manifesta que el dret de desconnexió digital no és un dret fonamental**

  Els incompliments en els quals va incórrer l'empresa van comportar que el treballador es vera exposat a jornades molt prolongades i en horaris intempestius, van poder comprometre el seu dret al descans i a la desconnexió digital, la qual cosa ha pogut incidir en el procés d'incapacitat temporal en el qual es troba, però tals incompliments, si bé generen dret a extingir voluntàriament el contracte de treball amb la indemnització corresponent, no generen una indemnització addicional de danys i perjudicis perquè no s'han vulnerat drets fonamentals. El dret al descans i a la limitació del temps de treball apareixen en l'article 40.2 CE dins dels principis rectors de la política social i econòmica, però no dins del capítol dedicat als drets fonamentals.

  Pots consultar la Sentència en este enllaç.