DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern nº 13 | Juliol 2021

DIRECTRIUS PER A LA CORRECTA UTILITZACIÓ DE XARXES SOCIALS CORPORATIVES

Í N D E X

DIRECTRIUS PER A LA CORRECTA UTILITZACIÓ DE XARXES SOCIALS CORPORATIVES

Vos convidem a traslladar-nos les temàtiques que resulten de vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUSCRIPCIONS

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

enllaç

"A DIFERÈNCIA DELS LLOCS WEB GESTIONATS DIRECTAMENT O INDIRECTAMENT PER LES PRÒPIES ADMINISTRACIONS PÚBLIQUES, I SOBRE ELS QUALS ÉS POSSIBLE UN CONTROL TOTAL DEL CONTINGUT I DE LA MENA DE SERVEI PRESTAT, LA XARXA SOCIAL ÉS UN ENTORN QUE NO ESTÀ PENSAT INICIALMENT PER A L'ÚS ADMINISTRATIU. EN QUALSEVOL CAS, SUPOSA UN TRACTAMENT DE DADES PERSONALS QUE HA DE COMPLIR AMB LA NORMATIVA DE PROTECCIÓ DE DADES".

INTRODUCCIÓ

Les xarxes socials són un dels canals d'informació més usats en Internet. Els usuaris troben en elles un canal senzill, accessible i immediat pel qual poden compartir continguts, socialitzar o fins i tot oferir un aparador per a donar a conéixer els seus productes o serveis.

La relació de les Administracions Públiques amb les xarxes socials pot prendre moltes formes. La més coneguda seria la presència de perfils 'oficials' dels organismes en xarxes socials obertes, encara que no poden obviar-se altres usos com les xarxes socials tancades utilitzades com a vehicle de comunicació interna, les xarxes o grups no oficials d'empleats, o els empleats que publiquen en xarxes socials a títol individual.

A diferència dels llocs web gestionats directament o indirectament per les pròpies Administracions Públiques, i sobre els quals és possible un control total del contingut i de la mena de servei prestat, la xarxa social és un entorn que no està pensat inicialment per a l'ús administratiu.

En qualsevol cas, la seua utilització suposa un tractament de dades personals que ha de complir amb la normativa de protecció de dades.

A continuació, s'ofereixen una sèrie de directrius per al correcte ús de les xarxes socials corporatives, tant de manera interna com per a l'oferta de serveis als ciutadans. Així mateix, es farà un repàs a alguns dels principals riscos per als drets i llibertats dels interessats, associats a l'ús de les xarxes socials.

ÚS DE XARXES SOCIALS DE MANERA INTERNA

En l'ús intern de les xarxes socials, podem trobar-nos amb xarxes tancades, pensades per als empleats com una evolució de les intranets corporatives a les quals s'han afegit trets socials. Aquestes xarxes es recolzen en paquets de programari específic i l'accés està restringit o fins i tot prohibit a tercers.

Un altre possible ús intern de les xarxes socials és el que resulta de les comunicacions informals dels empleats, que formen grups per a parlar o intercanviar missatges i notícies. Aquest tipus de xarxes a vegades sorgeix de manera espontània i altres vegades pot ser promogut per les pròpies organitzacions. Ens podem trobar amb empleats d'una mateixa entitat (i a vegades també juntament amb antics empleats i externs) que tracten assumptes professionals entre ells a través d'una xarxa insegura sense ser, moltes vegades, conscients d'això. Un empleat, de manera inconscient i sense valorar els riscos que representa, pot arribar fins i tot a confondre la xarxa social de companys amb la intranet o els canals interns establits i publicar documents, estratègies o dades corporatives que poden ser accessibles, i fins i tot fàcilment copiats, per tercers no autoritzats. Al seu torn, aquest empleat també podria publicar opinions o fer comentaris de tipus eminentment personal que un lector malintencionat podria fer passar per oficials. En aquest mateix context i estretament relacionat, l'AEPD s'ha fet eco en diverses ocasions del perill que poden representar els grups d'empleats i els comentaris abocats en ells en situacions d'assetjament laboral, sexual i casos de discriminació.

"ELS LÍMITS D'USOS DE XARXES SOCIALS HAN DE QUEDAR CLARAMENT DEFINITS EN LA POLÍTICA INTERNA DE L'ENTITAT. SI EN LA POLÍTICA S'ADMETEN AQUEST TIPUS DE CANALS DE COMUNICACIÓ, S'ESTÀ ADMETENT UN TRACTAMENT DEL QUAL SERÀ RESPONSABLE L'ENTITAT I, PER TANT, HAURÀ DE COMPLIR AMB ELS ESTABLIT EN EL RGPD I EN L'ENS".

Els límits d'usos de xarxes socials han de quedar clarament definits en la política interna de l'entitat . Si en la política s'admeten aquest tipus de canals de comunicació, s'està admetent un tractament del qual serà responsable l'entitat i, per tant, haurà de complir amb els establit en el RGPD i en l'ENS.

"EN LA POLÍTICA D'INFORMACIÓ DE L'ENTITAT HA DE QUEDAR CLAR, ALMENYS DES DE LA PERSPECTIVA DE PROTECCIÓ DE DADES, LA PROHIBICIÓ DE REALITZAR EL TRACTAMENT DE DADES PERSONALS RELATIVES A L'ACTIVITAT DE L'ENTITAT A TRAVÉS DELS PERFILS PERSONALS EN LES XARXES SOCIALS PARTICULARS DELS EMPLEATS".

EMPLEATS QUE PUBLIQUEN EN XARXES SOCIALS DE MANERA INDIVIDUAL

També és bastant comú que professionals publiquen continguts en xarxes socials aportant la seua experiència al coneixement comú. En algunes organitzacions és freqüent fins i tot que es promoga l'ús de les xarxes socials pels experts de l'entitat .

No obstant això, que els empleats publiquen informació professional pot infringir els principis de protecció de dades, quan s'inclou informació personal i es manca de legitimació.

Per això, en la Política d'Informació de l'entitat ha de quedar clar, almenys des de la perspectiva de protecció de dades, la prohibició de realitzar el tractament de dades personals relatives a l'activitat de l'entitat a través dels perfils personals en les xarxes socials particulars dels empleats.

L'ÚS DE XARXES SOCIALS PER A L'OFERTA DE SERVEIS ALS CIUTADANS

El 'Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics', estableix com a canal d'assistència per a facilitar l'accés de les persones interessades als serveis electrònics proporcionats en el seu àmbit competencial, entre altres, el de les xarxes socials.

Ara bé, **quan una Administració Pública decidisca oferir informació o serveis als ciutadans a través d'una xarxa social, no pot obligar l'administrat a comptar amb perfils en aquesta**, en la mesura en què aquestes xarxes realitzen tractaments addicionals de dades basades en el consentiment de l'usuari. Per exemple, realitzar iniciatives de participació ciutadana únicament a través de xarxes socials obliga a aquells subjectes que vulguen tindre influència en aquesta iniciativa a consentir en el tractament d'un tercer i, en conseqüència, a atorgar un consentiment que podria no complir els requisits del RGPD.

"EL SERVEI PROPORCIONAT MITJANÇANT LA XARXA SOCIAL HAURÀ DE COMPLIR AMB TOTES LES OBLIGACIONS ESTABLIDES EN EL RGPD, ENTRE ELLES EL DEURE D'INFORMAR".

El servei proporcionat mitjançant la xarxa social haurà de complir amb totes les obligacions establides en el RGPD, entre elles el deure d'informar. Aquesta obligació podria implementar-se en un post fixat a l'inici del compte de manera que l'usuari puga accedir fàcilment i que proporcionara la política de privacitat o un enllaç a aquesta.

LEGITIMACIÓ

El tractament de les dades per part de les xarxes en la qual els usuaris disposen de compte es basarà, en general, en aquells necessaris per a l'execució del contracte de servei o en el consentiment prestat. Cal distingir aquestes causes de legitimació de les d'aquells tractaments de les dades dels ciutadans realitzats per les Administracions Públiques amb perfil en les xarxes socials derivats de la interacció amb les persones arran de la informació proporcionada per l'Administració a través del seu compte oficial i la legitimació del qual per a ser tractats per l'Administració estaria basada en el compliment d'una missió realitzada en interés públic o en l'exercici dels poders públics conferits.

COOKIES

El tractament de dades realitzat per la xarxa social podria incórrer en la recollida d'un volum major de dades personals del ciutadà dels necessaris per part de l'Administració Pública en la gestió del seu perfil oficial o de dades addicionals que no tinguen cap relació amb aquesta gestió. El rol que l'Administració Pública i la xarxa social exerceixen respecte al tractament de les dades personals recollits podria canviar a corresponsables depenent de si l'Administració Pública no és diligent per a conéixer aquesta circumstància, o, coneixent-los, té opcions per a configurar o limitar el tractament que realitza la xarxa social i no fa ús d'ells, o permet activament que es produïsca el tractament. Per exemple, en cas dels ginys a les xarxes socials incloses en els portals de les Administracions, abans de permetre l'ús de cookies per aquests recursos, és necessari que les Administracions recapten el consentiment previ del

DEURE D'INFORMAR

"L'ENTITAT HA DE DISPOSAR D'UNA POLÍTICA DE COMUNICACIÓ EN XARXES SOCIALS QUE REFLECTISCA ASPECTES DE LA POLÍTICA DE PROTECCIÓ DE DADES DE L'ENTITAT".

visitant dels seus pàgines, mantenint els ginys deshabilitats fins a la seua obtenció.

POLÍTICA DE COMUNICACIÓ EN XARXES SOCIALS

L'entitat ha de disposar d'una política de comunicació en xarxes socials que reflectisca aspectes de la Política de Protecció de Dades de l'entitat com són:

- Una responsabilitat clara i embeguda de manera eficient en la cadena de responsabilitats de l'entitat , de manera que la comunicació per la xarxa o xarxes socials estiga ben alineada amb la resta de la política de comunicació institucional.

- Un document informatiu per als empleats públics on s'indique què poden fer i què no en la xarxa social de l'Administració. Si es parteix de la base que les xarxes socials són un suport o complement a una pàgina web i una seu oficial, és més fàcil limitar el servei i evitar riscos.

- Una formació adequada a les persones encarregades de publicar continguts i atendre comentaris i qüestions.

PERFILAT DELS USUARIS

Les xarxes socials poden ser un mitjà perquè les Administracions coneguen dades estadístiques dels seus usuaris, a través de la informació que proporciona la pròpia plataforma. Això podria realitzar un perfilat dels usuaris, dels seus interessos i de les seues tendències de navegació. En la mesura en la qual involucren tractaments de dades personals, a més d'estar legitimat, especialment quan de la navegació es poden inferir categories especials de dades, s'ha de proporcionar informació d'aquests tractaments de conformitat amb els articles 13 i 14 del RGPD.

"EL CONTINGUT DE TERCERS, INSERIT COM A ANUNCIS O D'UNA ALTRA FORMA, POT PORTAR A ENGANY ALS USUARIS I FER CREURE A AQUESTS QUE SÓN ENLLAÇOS QUE PERTANYEN A SERVEIS DE L'ADMINISTRACIÓ PÚBLICA QUE RECAPTEN DADES PERSONALS, PER LA QUAL COSA AQUESTS CONTINGUTS HAN D'ESTAR SOTA SUPERVISIÓ O CONTROLAR EL TIPUS DE CONTINGUTS QUE ES POT OFERIR, EN PARTICULAR, CONTINGUTS RELACIONATS AMB IDEOLOGIES I CREENCES DE QUALSEVOL ÍNDOLE".

RISCOS PER ALS DRETS I LLIBERTATS DELS CIUTADANS ASSOCIATS A LES XARXES SOCIALS

Una vegada que s'ha dissenyat un tractament a través de xarxes socials que complisca amb els requisits establits en el RGPD, és necessari analitzar els riscos que per als drets i llibertats dels ciutadans es poden originar, amb la finalitat de dur a terme la gestió adequada d'aquests.

Alguns d'aquests riscos són:

- Que es produïsquen errors en l'aplicació de les polítiques de comunicació a través de xarxes socials que revelen dades de caràcter personal de manera indesitjada tant dels administrats com dels propis empleats públics (publicació de CSV, metadades...). Per a reduir el risc és necessària la definició d'una política interna clara i ben coneguda pel personal sobre les implicacions i conseqüències de la participació en xarxes socials.

- Els comptes oberts en una xarxa social per una Administració Pública poden veure's compromeses i per tant es pot infiltrar contingut en elles amb el propòsit de recaptar dades de caràcter personal. Això ha de ser tingut en compte a l'hora de gestionar els processos d'assignació i renovació de claus d'accés.

- D'altra banda, el contingut de tercers, inserit com a anuncis o d'una altra forma, pot portar a engany als usuaris i fer creure a aquests que són enllaços que pertanyen a serveis de l'Administració Pública que recapten dades personals, per la qual cosa aquests continguts han d'estar sota supervisió o controlar el tipus de continguts que es pot oferir, en particular, continguts relacionats amb ideologies i creences de qualsevol índole.

- En el cas que es proporcionen espais als administrats per a pujar els seus propis continguts, es recomana evitar que la publicació d'aquests continguts es realitze sense supervisió per a evitar la divulgació d'informació personal de tercers sense el seu consentiment, en particular,

contingut sensible o qualsevol conducta que tinguera implícits actes de violència digital.

- En cas que, per a l'accés als continguts de la xarxa social, es requerisca iniciar una sessió per part de l'administrat, l'Administració Pública ha d'avaluar les garanties de privacitat, incloent les mesures de seguretat orientades a la privacitat que proporciona aquesta xarxa, especialment la política de creació d'usuaris i contrasenyes. Aquesta anàlisi ha de realitzar-se en interés dels ciutadans, però també en la dels gestors de l'espai podent un atacant suplantar als publicadors.

- De cara a les responsabilitats assumides per les Administracions i relacionat amb les tecnologies de seguiment (cookies), és preferible que en el lloc web de l'Administració, o en les *newsletters* que en el seu cas es distribuïsquen, s'incloguen enllaços estàtics al perfil oficial en la xarxa social, enfront de l'ús de ginys embeguts en el contingut.

- Les tècniques actuals no sempre permeten determinar amb total efectivitat que l'usuari puga ser un menor d'edat. Caldrà avaluar el risc que això suposa en relació amb la mena de continguts que s'estan oferint a través de la xarxa i, en funció d'aquest risc, establir procediments addicionals per a la comprovació més precisa de l'edat dels usuaris.

"EN CAS QUE, PER A L'ACCÉS ALS CONTINGUTS DE LA XARXA SOCIAL, ES REQUERISCA INICIAR UNA SESSIÓ PER PART DE L'ADMINISTRAT, L'ADMINISTRACIÓ PÚBLICA HA D'AVALUAR LES GARANTIES DE PRIVACITAT, INCLOENT LES MESURES DE SEGURETAT ORIENTADES A LA PRIVACITAT QUE PROPORCIONA AQUESTA XARXA, ESPECIALMENT LA POLÍTICA DE CREACIÓ D'USUARIS I CONTRASENYES".

MATERIAL COMPLEMENTARI

- Tecnologies i Protecció de Dades en les Administracions Públiques (AEPD). Consulta en aquest enllaç.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics. Consulta en aquest enllaç.
- Guia de Comunicació Digital per a l'Administració General de l'Estat. Fascicle 8. Consulta en aquest enllaç.
- 'Mesures de seguretat en Facebook' (AEPD). Consulta en aquest enllaç.
- Bones pràctiques en Xarxes Socials. (CCN-CERT). Consulta aquest enllaç.
- Protegeix el teu perfil corporatiu en xarxes socials amb aquests consells del CCN (CCN-CERT). Consulta aquest enllaç.

NOTÍCIES

- **Nou formulari de notificació de bretxes de dades personals.**

  L'Agència Espanyola de Protecció de Dades ha actualitzat el formulari habilitat perquè els responsables dels tractaments de dades personals complisquen amb la seua obligació de notificar les bretxes que s'hagen produït. Aquest nou sistema simplifica la notificació de bretxes de dades personals guiant als responsables a través de preguntes concretes, de manera que els responsables coneguen els punts que han d'abordar en aquesta.

  Consulta més detalls en aquest enllaç.

- **L'AEPD publica una nova guia per a gestionar el risc dels tractaments de dades personals i realitzar avaluacions d'impacte.**

  L'Agència Espanyola de Protecció de Dades ha publicat la guia 'Gestió del risc i avaluació d'impacte en tractaments de dades personals', un document que incorpora l'experiència acumulada en l'aplicació de la gestió del risc en l'àmbit de la protecció de dades des de l'aplicació del Reglament General de Protecció de Dades (RGPD) i afig les interpretacions de l'AEPD, el Comité Europeu de Protecció de Dades i el Supervisor Europeu de Protecció de Dades.

  El document, dirigit a responsables, encarregats de tractaments i delegats de protecció de dades (DPD), ofereix una visió unificada de la gestió de riscos i de les avaluacions d'impacte en protecció de dades, i facilita la integració de la gestió de riscos en els processos de gestió i governança de les entitats.

  Consulta la Guia en aquest enllaç.