PÍNDOLA 39.- Riscos relatius a la protecció de dades en l'ús de tecnologies per part de les administracions públiques

En aquesta píndola es fa un resum de la Guia de Tecnologies i Protecció de Dades en Administracions Públiques publicada per l'Agència Espanyola de Protecció de Dades (AEPD), que analitza un conjunt de tecnologies senyalant algun dels riscos relatius a la protecció de dades que les administracions públiques, com a responsables, han de tenir en compte a l'hora d'incorporar-les com a suport als tractaments que realitzin; així com aquelles mesures tècniques i organitzatives que permetin eliminar o mitigar a un nivell acceptable els danys als drets i llibertats de les persones que puguin derivar-se del tractament.

En concret, s'analitzen alguns dels aspectes específics de compliment i dels riscos que poden aparèixer en els tractaments derivats de l'ús d'aquestes tecnologies: **cookies** i tecnologies de seguiment, **xarxes socials, cloud computing, big data, intel·ligència artificial, blockchain** i tecnologies de registre distribuït, i **smart cities**.

I.

El seguiment de l'activitat dels usuaris en la xarxa s'implementa mitjançant dispositius anomenats **Cookies**. El responsable del portal ha **d'informar i comprovar** quin tipus de *cookies* requereix el gestor de continguts i els *plugins* que es vulguin utilitzar, de manera que **s'eliminin aquelles no necessàries** per prestar el server i optant per aquells gestors de continguts que facin ús de *cookies* tècniques pròpies. D'altra banda **el rebuig a l'ús de *cookies*** no imprescindibles per a la implementació del servei no pot suposar un **impediment per accedir** al portal de l'administració pública.

En el cas d'utilitzar tecnologies per realitzar **anàlisi de trànsit** es convenient seguir el principi de **minimització** de dades i recollir les dades de navegació de forma anonimitzada o pseudonimitzada. En cas de recórrer a **eines de tercers** amb aquesta finalitat, han d'estudiar-se les diferents alternatives que ofereix el mercat, analitzar les característiques tècniques i maneres de funcionament per evitar possibles incompliments normatius. En aquest sentit l'eina **Google Analytics resulta especialment problemàtica** en relació als estàndards de protecció de dades ja que les adreces IP dels usuaris s'emmagatzemen en servidors ubicats en els Estats Units i de forma pseudonimitzada. Es recomana tenir en compte eines alternatives com ara https://matomo.org/, o https://www.econda.de/en/.

II.

Les **xarxes socials**, no estan pensades per usos administratius, tot i que les administracions públiques les utilitzen com a eina per fer-se eco de la informació oficial i proporcionar informació àgil als usuaris. En qualsevol cas suposen un tractament que ha de complir amb l'establert en l'RGPD. També es poden utilitzar xarxes socials **tancades** com a vehicle de **comunicació interna** entre empleats.

En el cas d'oferir informació o serveis als ciutadans a través d'una xarxa social oberta (Facebook, Instagram, Twitter, etc.) sense proporcionar canals alternatius, el **consentiment no podrà ser considerat lliure** i no complirà amb els **requisits** que exigeix l'RGPD, a demés de suposar un obstacle. El servei proporcionat a través de la xarxa social haurà de complir amb totes les obligacions establertes en l'RGPD, entre elles la **d'informar** sobre la **política de privacitat**.

La majoria de xarxes socials **no ofereixen nivells de qualitat** de servei contrastats per a que puguin esdevenir instruments de notificació, **tampoc existeixen garanties de confidencialitat** en la transmissió d'informació a través de la xarxa social.

LES PÍNDOLES DEL DPD

III.

La computació al núvol, o **Cloud Computing**, és una forma d'utilitzar servidors en localitzacions remotes d'una manera flexible i transparent, en comptes d'emprar equips propis comprats i allotjats en instal·lacions corporatives, utilitzant equips o serveis virtuals gestionats remotament. Atenent al tipus de serveis oferts, podem distingir entre solucions d'Infraestructures com a Servei (**IaaS**), Plataformes com a Servei (**PaaS**) y Software com a Servei (**SaaS**). Un altre possible classificació dels núvols és la separació entre públics (quan es proporcionen diversos serveis a diferents clients) i privats (quan el proveïdor ofereix una sèrie de serveis agrupats i de forma tancada a tercers).

La contractació d'un servei al núvol no suposa un desplaçament total de les obligacions de gestió de la seguretat a l'encarregat del tractament sinó que correspon sempre al **responsable del tractament** la presa de decisions amb relació als requisits de protecció de dades personals, que hauran de comptar amb els **requisits que s'estableixen a l'article 32 del RGPD**.

Per evitar produir-se una infracció de la normativa de protecció de dades, el **responsable** ha d'escollir a un encarregat que **ofereixi garanties**, oferint-li, a través d'un contracte, les **instruccions i maneres de procedir** quan realitzi tractaments de **dades personals.** L'administració també ha de **gestionar els riscos** en cas que el proveïdor del núvol decideixi **discontinuar el servei** o canviar les condicions en que es presta, així com el risc legal de que existeixin **canvis normatius** o d'altres naturaleses que impedeixin la utilització dels serveis. En aquest sentit s'han de desenvolupar mesures i plans de contingència de **migració dels serveis** a altres sistemes.

IV.

El **Big Data**, o tractament massiu de dades, fa referència a grans conjunts de dades, caracteritzats pel seu volum, varietat, velocitat i variabilitat, que requereixen d'una tecnologia escalable per a un emmagatzematge, manipulació, gestió i anàlisi eficient. Des del punt de vista de protecció de dades personals, és important assegurar-se que existeix una **legitimació** per aquest tipus de tractaments massius de dades, i en el cas que s'incloguin **categories especials de dades** és necessari aixecar prèviament la **prohibició** per al seu tractament. Per tant per a **reutilitzar les dades** en nous projectes resulta clau realitzar un anàlisi de no incompatibilitat i la **prèvia realització d'una avaluació d'impacte** que haurà de tenir en compte una sèrie de **consideracions per minimitzar els riscos** que el tractament pugui suposar pels drets i llibertats de les persones, adoptant una sèrie de garanties en el disseny:

- **Fase d'adquisició de dades:** minimitzar les dades tractades seleccionant-les prèviament a la recollida i el grau de detall emprant tècniques d'anonimització / pseudonimització.
- **Fase d'anàlisi i validació:** com en la fase anterior, minimitzar el detall de les dades mitjançant tècniques d'anonimització i xifrat.
- **Fase d'anonimització o pseudonimització:** les persones que realitzin aquesta fase no hauran de ser les mateixes que participen a la fase d'explotació de la informació. Aquesta recomanació esdevé obligatòria quan es tractin dades de salut.
- **Fase d'emmagatzematge:** s'ha de garantir la confidencialitat de les dades i que aquestes no siguin accessibles per tercers no autoritzats, emprant tècniques de xifrat i mecanismes d'autenticació i control d'accés.
- **Fase d'explotació:** quan s'utilitzin les dades per extreure valor i presentar la informació que derivi, haurà de garantir-se l'anonimització d'aquestes de cara a evitar la reidentificació.

El procés d'agregació també comporta riscos com la reidentificació, vinculabilitat i la inferència.

LES PÍNDOLES DEL DPD

V.

En relació amb la **Intel·ligència Artificial** o IA, en el cas d'una utilització massiva de dades per entrenar el sistema (*Machine Learning*), és convenient tenir en compte els mateixos riscos descrits en el cas dels tractaments basats en *Big Data*. En cas d'utilitzar **components de tercers**, com podria ser integrar en un sistema un motor d'IA extern que s'executés a Àsia rebent dades i retornar els resultats, cal tenir en compte que poden ser una font de riscos que s'han de gestionar. Si el tractament basat en IA pren decisions basades únicament en el tractament automatitzat de les dades explotades, és recomanable que els organismes públics analitzin els riscos que es derivin d'aquest mètode de presa de decisions i adoptin mecanismes per al seu anàlisi i gestió, i consultin prèviament al Delegat de Protecció de Dades.

VI.

En relació amb l'ús de tecnologia **blockchain,** abans de posar en marxa un projecte amb aquesta tecnologia ha d'analitzar-se la compatibilitat de la solució amb les exigències normatives imposades per el RGPD:

- **Responsabilitat del tractament**: en un sistema descentralitzat és difícil identificar al responsable del tractament.
- **Dret a l'oblit i rectificació**: la impossibilitat d'alterar el contingut sense produir una inconsistència provoca que l'existència de solucions per eliminar o modificar la informació registrada s'hagi d'analitzar cautelosament.
- **Conservació limitada de les dades**: és necessari implementar mecanismes alternatius que donin solució a la immutabilitat pròpia de la xarxa de manera que les dades personals es mantinguin durant no més temps del necessari per dur a terme les finalitats del tractament.
- **Seguretat**: dos aspectes de seguretat importants són la confidencialitat de les dades a l'exposar-se informació a la xarxa, i la no garantia de la disponibilitat dels nodes.
- **Transferències internacionals de dades**: la naturalesa de les xarxes *blockchain* públiques fa possibles les transferències internacionals de dades. Es recomana escollir una xarxa *blockchain* privada o híbrida així com un model d'emmagatzematge *off-chain* de les dades.

Addicionalment, l'article 3 del Real Decreto-ley 14/2019 del 31 d'octubre, preveu que en les relacions dels interessants amb les administracions públiques **no seran admissibles** en cap cas, ni podran ser autoritzats, els **sistemes d'identificacions** basats en tecnologies de registre distribuït ni els sistemes de firmes basats en els anteriors, en tant que **no siguin objectes de regulació específica** per l'Estat en el marc del Dret de la Unió Europea.

De cara a escollir la implementació *blockchain* s'ha d'avaluar si la solució tecnològica adoptada és la més adequada, **privacitat des de el disseny**, si introdueix riscos que no permeten ser gestionats, avaluar quin **tipus d'arquitectura de xarxa *blockchain*** s'adapta millor a la solució: públiques, privades, permissionades (permetent a una autoritat central conservar l'accés als blocs i a les dades) o no permissionades. En tot cas, es recomana consultar prèviament al Delegat de Protecció de Dades.

VII.

Finalment, en els projectes per a la instal·lació de sensors/actuadors de forma massiva cal considerar que s'incrementa la probabilitat de que es produeixin fallades de seguretat en els dominis de la **confidencialitat, disponibilitat i integritat** en el cas de recollir dades personals. Aquest tipus de projectes requereixen d'un anàlisi de riscos i de la consulta prèvia al Delegat de Protecció de Dades.

Per a més informació:

- Guía Tecnologías y Protección de Datos en Administraciones Públicas:
  https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.)