EAPC - Gestió de la informació: transparència i protecció de dades

La protecció de dades més enllà de la intimitat

24-10-2022

És força freqüent que s'associï la protecció de dades personals a la protecció de la intimitat de les persones. Tant és així que sovint hi ha qui es pregunta: "**per què m'he de preocupar de la protecció de les dades personals si no tinc res a amagar?**". En altres termes, es formula un plantejament en el sentit que si a algú no li preocupa gaire preservar la seva intimitat, la protecció de dades és quelcom que no l'afecta. Però aquesta pregunta, i el plantejament que li és inherent, és reduccionista almenys per un triple motiu: fa referència únicament a si es té quelcom a amagar –confidencialitat– i no atorga cap valor a les dades, probablement no som conscients de l'ús que se'n pot fer, ni de com ens pot afectar en el nostre dia a dia.

Les dades personals poden transmetre més informació de la que inicialment coneixem

Quan una persona considera que "no té res a amagar" ho fa valorant succintament la que considera que és informació sensible en relació amb la seva persona, però òbviament aquesta anàlisi se circumscriu a la informació que "coneix" en un context present i, per tant, sense poder valorar ni la informació que desconeix ni la que eventualment pot aflorar mitjançant l'ús d'una nova tecnologia.

Imaginem que es tracta d'una persona sense cap patologia coneguda i, en considerar que en aquell moment "no té res a amagar", autoritza la divulgació pública de les seves rutes (*tracks*) en bicicleta juntament amb les mesures cardíaques. Potser la decisió hauria estat una altra si hagués sabut que a partir d'aquesta informació es podia observar que patia una malaltia cardíaca.

També hauria pogut succeir que al cap d'un temps de compartir públicament aquesta informació aparegués una nova tecnologia que permetés identificar malalties cardíaques basant-se en la informació referida. Si s'hagués anticipat que a partir d'aquelles mesures de batecs del cor aparentment irrellevants en el futur es podria obtenir aquella conclusió, segurament la decisió sobre la seva divulgació hauria estat diferent.

En ambdós escenaris la conseqüència pot ser significativa i, per exemple, pot fer que potencials ocupadors optin per altres candidats a la vista d'aquesta informació que s'hauria fet pública.

En definitiva, cal ser especialment cautelosos de menystenir la protecció de les nostres dades personals, ja que és possible que **les nostres dades personals ens exposin més del que havíem pogut preveure**.

Les múltiples dimensions de seguretat de les dades personals

L'Esquema Nacional de Seguretat (ENS) estipula que cal protegir diverses dimensions de seguretat de les dades. Aquesta aproximació multidimensional ens ajuda a mostrar que les dades personals són més que la "intimitat", atès que el seu tractament pot afectar molts aspectes de la nostra vida privada. En concret, les dimensions que estableix l'ENS són:

- a) **Confidencialitat**: propietat o característica consistent que **la informació ni es posa a disposició, ni es revela** a individus, entitats o processos no autoritzats.
- b) **Integritat**: propietat o característica consistent que la informació **no ha estat alterada** sense autorització.
- c) **Traçabilitat**: propietat o característica consistent que **les actuacions** d'una entitat (**persona** o procés) **poden ser traçades de manera indiscutible** fins a aquesta entitat.
- d) **Autenticitat**: propietat o característica consistent que **una entitat és qui diu ser** o bé que garanteix la font de la qual procedeixen les dades.
- e) **Disponibilitat**: propietat o característica dels actius consistents que les entitats o els processos autoritzats hi tenen **accés** quan ho requereixin.

Quan s'associa implícitament protecció de dades a intimitat, s'està reduint la protecció de dades a una única de les dimensions indicades: la confidencialitat. No obstant això, tal com es pot constatar, hi ha almenys fins a quatre dimensions de seguretat addicionals. El motiu és que, tal com s'explicarà en l'apartat següent, les dades constitueixen un mitjà –crític– per dur a terme diferents funcions i, per protegir efectivament aquestes funcions, cal preservar les dades des de múltiples dimensions.

Reduir la protecció de dades a la protecció de la dimensió "confidencialitat" equivaldria a considerar que mentre no es divulgui indegudament la informació és indiferent que la informació:

- sigui alterada indegudament,
- no es puguin atribuir les actuacions a persones concretes,
- no sigui possible verificar les identitats i
- no resulti accessible.

Les dades personals com a mitjà

El principal motiu pel qual es consideren –i es protegeixen– les diferents dimensions de seguretat indicades és que les dades tenen més utilitat que la d'emmagatzemar informació "privada".

De fet, continuant en l'entorn de les dades de salut, imaginem que únicament es protegeix la dimensió "confidencialitat":

- Si les dades es poden modificar indegudament, per exemple per part d'un *hacker* extern, hi hauria un risc significatiu per als usuaris de la sanitat, ja que es podrien alterar històries clíniques i subministrar medicaments erròniament o intervenir quirúrgicament de malalties diferents de les realment patides pels pacients.
- En cas que les actuacions no es puguin atribuir adequadament (no hi hagi traçabilitat), fallaria tot el sistema de permisos, de manera que personal sanitari no qualificat podria efectuar modificacions per a

les quals no estaria autoritzat.

- En el supòsit que no es puguin verificar les identitats i l'origen de les dades, el sistema informàtic deixaria de ser confiable, ja que si no es pot conèixer amb certesa l'origen de la informació –independentment que la dada resti immutable– perd la seva utilitat i generaria una gravíssima distorsió en el sistema. Només cal imaginar que en les dades del sistema sanitari s'haguessin introduït dades inventades i que no es poguessin distingir de les fiables (o en dades d'un banc, que s'haguessin introduït més saldos a diferents comptes).
- Finalment, també és crític –en atenció a l'ús de la informació– poder-ne disposar. Imaginem que un pacient entra a un hospital amb una malaltia que requereix una intervenció urgent i que té patologies prèvies. Poder accedir a la seva història clínica en aquell moment és crític.

En definitiva, la protecció de dades vetlla per una protecció integral de les persones i de la seva informació i, per tant, de les seves diferents dimensions, més enllà de la de la confidencialitat.

Però és que, en qualsevol cas, la protecció de la confidencialitat també presenta més implicacions que la de respectar o mantenir la intimitat de les persones. Així, si es produeix un accés indegut a informació que s'havia de mantenir confidencial, els riscos són múltiples, ja que qui accedeix la pot emprar per a múltiples finalitats i, un cop perdut el control de la informació, no es pot determinar ni limitar qui acabarà podent-hi accedir ni què en farà.

En resum, es constata que cal una protecció integral (que comprengui totes les dimensions) de les dades personals per assegurar una adequada protecció del conjunt de drets i llibertats de la ciutadania, ja que mitjançant el tractament de les dades personals s'hi pot incidir. En cas que per qualsevol circumstància aquesta protecció es vegi compromesa, qualsevol dret o llibertat es pot veure significativament afectat. No obstant això, a efectes il·lustratius, ens centrarem únicament en tres possibles conseqüències derivades de la pèrdua del control de les dades personals: discriminació, encapsulament o filtre bombolla i nous perjudicis.

- Discriminació: Suposem que una persona no té inconvenient a compartir públicament a les xarxes socials les seves conviccions religioses. No obstant això, anys més tard vol viatjar a un país on –imaginem– no es permet l'entrada a les persones amb aquestes creences religioses.

Aquest exemple il·lustra com un cop divulgada aquesta informació personal –o qualsevol altra-, és difícil garantir que no ha estat recopilada o consultada per algú que la pugui emprar en contra nostra, en particular per discriminar-nos.

- Encapsulament / filtre bombolla: Un dels usos més freqüents que es duen a terme a partir de la recopilació de dades personals consisteix a confeccionar un perfil dels usuaris. D'acord amb els referits perfils es poden tant dissenyar estratègies de publicitat especialment adreçades a un segment concret, com directament emprar aquests perfils per filtrar la informació a mostrar i que, en conseqüència, serà diferent en funció de cadascun dels usuaris (o de la tipologia/perfil a la qual cada usuari hagi estat assignat).

En conseqüència, imaginem que algú accepta divulgar les seves preferències polítiques (per cert, fàcilment deduïble a través de xarxes socials i la recerca que es pot dur a terme mitjançant diverses fonts d'informació obertes) o que així ho ha inferit un determinat cercador d'internet.

A partir de les preferències identificades, el cercador mateix opta per mostrar-li sempre les notícies més coincidents amb la seva preferència ideològica (ja que la probabilitat que les llegeixi és superior i així podrà recopilar encara més dades i mostrar més anuncis).

No obstant això, l'usuari afectat –sense saber-ho– s'haurà vist encapsulat, ja que no tindrà accés (o únicament de manera residual) a informació alternativa a la preferència inicialment mostrada o deduïda. En conseqüència, la seva llibertat per canviar eventualment de pensament o preferència es veurà significativament minvada.

- Nous perjudicis: La divulgació o accés indegut a dades personals com podrien ser contrasenyes (fins i tot biomètriques) o dades de geolocalització comporten un risc no només per la vulneració de la intimitat del ciutadà sinó també perquè aquella informació pot ser emprada per dur a terme altres accessos indeguts, ja sigui als comptes del banc –en cas que s'empri la mateixa contrasenya– o al domicili mateix aprofitant que la família està de vacances (circumstància deduïda a partir de les dades de geolocalització). En definitiva, la fuita de dades personals pot no només generar una afectació sinó tenir una cadena d'implicacions en diferents àmbits.

El valor intrínsec de les dades

Considerar que si "no tinc res a amagar" no és necessari preocupar-se de les dades personals d'un mateix implica, més enllà de tot el que s'ha exposat, una desatenció del valor de quelcom que és nostre.

Hi ha molts exemples que denoten el valor i la importància de les dades (i en particular de les dades personals). Un d'aquests exemples consisteix a apreciar com la disponibilitat de dades ha marcat els principals avenços en la intel·ligència artificial fins al punt que el factor que els ha desencadenat ha estat més la disponibilitat de les dades –juntament amb les possibilitats del seu tractament mitjançant la convergència de diferents tecnologies– que no la descoberta de nous algoritmes (afirmació formulada per Oriol Vinyals en el marc de la sessió "AI & BIG DATA CONGRESS 02: Keynote speaker. Deep Learning Toolbox en el 2020").

Tan important és el valor de les dades que l'Autoritat Catalana de la Competència fa sis anys va recomanar en el document "L'economia de les dades. Reptes per a la competència" que en l'àmbit de la contractació pública no es tingués en compte únicament el preu monetari (és la referència dels llindars) sinó la importància en termes de cessió de dades. I és que un contracte important pot tenir un valor monetari zero, però ser especialment rellevant en les prestacions intercanviades entre l'Administració i l'operador privat corresponent.

En definitiva, pot succeir el que és habitual en els usuaris: rebre prestacions i serveis a canvi, exclusivament, d'entregar les nostres dades personals.

No obstant això, aquesta apreciació en cap cas no hauria de conduir a pensar, tal com va alertar l'EDPS en l'Opinió 4/2017, que les dades personals són una simple mercaderia com ho poden ser els diners.

La necessitat d'una visió omnicomprensiva de la protecció de dades

No és adequat identificar de manera exclusiva la protecció de dades amb el dret a la intimitat. De fet, es tracta de dos drets diferents i, mentre el dret a la intimitat és un dret específic, el dret a la protecció de dades és un dret transversal que es projecta envers molts altres drets ja que actua, en certa manera, com escut protector.

En aquest mateix sentit, múltiples sentències del Tribunal Constitucional han apuntat que l'origen del dret a la protecció de dades està l'article 18.4 de la CE: "La llei ha de limitar l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici

dels seus drets". És a dir, que s'erigeix com un límit a determinats usos informàtics per garantir el conjunt dels drets que ens són propis (si bé el dret a la protecció de dades personals comprèn les dades encara que no es tractin de manera automatitzada).

La protecció de dades és el dret que ha de permetre evitar discriminacions, preservar la llibertat individual (per exemple, no trobant-se en un filtre bombolla), així com procurar per molts altres aspectes clau en la nostra societat, com pot ser la protecció dels nostres actius econòmics.

Es fa difícil avui dia pensar en qualsevol aspecte a protegir que no requereixi una adequada salvaguarda de les dades personals. En conseqüència, prescindir de la protecció de dades implica descuidar-ho tot: **les teves dades són els teus drets**.

La consolidació d'una societat basada en les dades exigeix establir uns fonaments sòlids en **la protecció de dades personals per tal de preservar eficaçment el conjunt de drets i llibertats dels seus ciutadans**.

Xavier Puig Soler

Auditor de Sistemes d'Informació de l'Autoritat Catalana de Protecció de Dades