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

Protecció de dades des del disseny i per defecte: una eina essencial per al model d'economia de dades

28-03-2022

Si els grans pilars en què es fonamenta el Reglament general de protecció de dades (RGPD) són el principi de responsabilitat proactiva i l'enfocament en el risc, la protecció de dades des del disseny i per defecte (PDDD) podem dir que és el paraigua sota el qual es poden agrupar els mecanismes que permeten donar resposta (i compliment) a aquests dos grans pilars.

El RGPD regula la PDDD en l'article 25, en els termes següents:

"1. Tenint en compte l'estat de la tècnica, el cost de l'aplicació i la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i de gravetat diversa que comporta el tractament per als drets i les llibertats de les persones físiques, el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, mesures tècniques i organitzatives adequades, com la pseudonimització, concebudes per aplicar de manera efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament, a fi de complir els requisits d'aquest Reglament i de protegir els drets dels interessats.

2. El responsable del tractament ha d'aplicar les mesures tècniques i organitzatives adequades amb la intenció de garantir que, per defecte, únicament es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament. Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a l'accessibilitat de les dades. Aquestes mesures han de garantir en particular que, per defecte, les dades personals no siguin accessibles, sense la intervenció de la persona, a un nombre indeterminat de persones físiques.

3. Es pot utilitzar un mecanisme de certificació aprovat d'acord amb l'article 42, com a element per acreditar el compliment de les obligacions establertes als apartats 1 i 2 d'aquest article."

Aquest concepte, ara obligació regulada, no és nou i va ser formulat per Ann Cavoukian als anys noranta. La privacitat en el disseny es basava en una sèrie de principis, que avui ens ajuden a entendre com aplicar-la en els nous requeriments establerts en l'article 25 del RGPD.

Els principis de la PDDD s'adrecen, principalment, a un objectiu: la prevenció. En aquest sentit, es busca identificar i aplicar les actuacions i mesures que ajudin a evitar que es produeixi un abús quan es tracten dades personals amb la finalitat de garantir els drets i les llibertats de les persones. Aquestes actuacions i mesures s'han d'aplicar tant en el moment de pensar què volem fer (quina activitat i tractament de dades) com al llarg de tota l'activitat, i s'han d'integrar en les tecnologies, l'arquitectura i les infraestructures i, també, en la forma d'organitzar i gestionar la informació.

Els principis desenvolupats per Ann Cavoukian són:

- prevenció i no correcció (proactivitat)
- privacitat per defecte (com a configuració predeterminada)
- privacitat integrada en el disseny
- funcionalitat plena (guanyar-guanyar)
- protecció de les dades en tot el seu cicle vital
- visibilitat i transparència
- respecte per la privacitat de l'usuari (*user centric*, 'centrat en l'usuari').

Aquests principis s'inclouen en el RGPD. D'una banda, en els considerants, com per exemple el considerant 78, que assenyala que aquestes mesures poden consistir, entre d'altres, a reduir al màxim el tractament de dades personals: pseudonimitzar com més aviat millor les dades personals; donar transparència a les funcions i al tractament de dades personals, i permetre als interessats supervisar el tractament de dades i al responsable del tractament crear i millorar elements de seguretat. De l'altra, la PDDD ha estat recollida en l'article 25 com una obligació específica, i també altres elements, com la responsabilitat proactiva i demostrable que ha d'inspirar totes les actuacions o la transparència respecte dels tractaments de dades que es porten a terme. La PDDD també es reflecteix en la resta d'obligacions, des de la creació i el manteniment del registre d'activitats de tractament fins a les avaluacions d'impacte sobre la protecció de dades o les notificacions de violacions de seguretat. Totes són mesures adreçades a millorar el control de les persones sobre les seves dades personals.

El Comitè Europeu de Protecció de Dades, en les Directrius 4/2019, relatives a la protecció de dades des del disseny i per defecte, emfasitza la rellevància que les mesures que s'adoptin siguin efectives i estiguin concebudes per aplicar els principis de protecció de dades i per integrar les garanties necessàries en el tractament de les dades. Aquestes mesures, tècniques i organitzatives, han de ser les adequades en funció del context i els riscos del tractament de les dades personals.

Això comporta que les mesures s'han de concebre perquè siguin sòlides i, si escau, aplicar mesures addicionals per anar-se adaptant als increments de risc que vagin sorgint (PDDD dinàmica). A més, recordem que el responsable del tractament ha d'estar en disposició de provar que els principis s'han complert i es mantenen. En el moment de fer aquestes valoracions, els elements que cal tenir en compte són:

- Estat de la tècnica: exigeix tenir en compte el progrés de la tecnologia disponible en el mercat. Per tant, cal avaluar de manera contínua els avanços tecnològics, no només els que puguin generar riscos, sinó també els que puguin ajudar a millorar el tractament.

- Cost de l'aplicació: cal valorar-ho tant en el moment de triar les mesures i les garanties com en el moment d'aplicar-les. No s'ha de destinar una quantitat desproporcionada de recursos si hi ha mesures alternatives menys costoses però que són efectives.

- Naturalesa, àmbit, context i finalitats del tractament: cal analitzar les característiques del tractament, la magnitud i la varietat de tractaments, les circumstàncies concretes i els objectius del tractament.
- Riscos de diversa probabilitat i gravetat: exigeix una avaluació sistemàtica i minuciosa del tractament, i tenir present que, en determinades casos, caldrà fer una avaluació d'impacte sobre la protecció de dades.

La PDDD, obligació regulada explícitament per a responsables del tractament, en el RGPD, i traslladable també als encarregats, amb la LOPDGDD, no es pot quedar aquí si es vol que les mesures que es puguin aplicar siguin realment efectives; és a dir, aquest "disseny" ha de formar part també de totes les activitats prèvies que puguin tenir impacte en el tractament de dades personals. La PDDD s'ha de convertir en imprescindible per a qualsevol entitat que tingui algun paper en l'ecosistema de les dades. Estem en un moment en què les tecnologies s'estan consolidant com a motor de la innovació i el desenvolupament de la societat, i això s'està fent basant-se en les dades de les persones, influint en totes les facetes dels éssers humans.

La quarta revolució industrial modifica el nostre entorn social, cultural, econòmic i polític, i configura un nou model de societat, on les persones estem vinculades directament a la producció d'informació. Aquesta realitat exigeix que la PDDD sigui un element estratègic de les organitzacions per configurar en entorn segur per a les persones. Exigeix anar més enllà de responsables i encarregats i mira a qualsevol que dissenyi, desenvolupi o produeixi productes i serveis, en qualsevol àmbit, que puguin acabar tractant informació personal. De fet, fins i tot en els productes i serveis que, en principi, no estan destinats a tractar dades personals, però sí que estan involucrats en l'economia de dades, potser caldria fer una anàlisi de riscos per valorar si, atenent al context, a la naturalesa, a les tecnologies utilitzades, etc., es podria arribar a produir una associació de la informació a una persona física, i si s'està en disposició d'implantar alguna mesura que millori el producte o servei, per reduir el risc que s'hagi pogut detectar.

A més, cal recordar que el principi de privacitat des del disseny, el de responsabilitat proactiva i el d'enfocament en el risc, exigeixen que tots els actors que conflueixen en la cadena de valor de les dades assumeixin la PDDD com a eina imprescindible per participar en el model que s'està creant al voltant de l'economia de les dades. Els que dissenyen i desenvolupen productes i serveis que han de comportar el tractament de dades personals, haurien d'adoptar la PDDD com a eina indissociable dels seus productes i serveis, ja que permetria als responsables i encarregats triar, amb més garanties, l'opció més idònia i efectiva per protegir els seus usuaris. I, en el cas de les administracions públiques, el RGPD en el considerant 78 indica expressament que els principis de la protecció de dades des del disseny i per defecte també s'han de tenir en compte en el context dels contractes públics.

La PDDD ens permetrà afrontar, de forma realista i pragmàtica, els reptes per als drets i les llibertats de les persones que es plantegen en un model de societat on la innovació es desenvolupa al voltant de la tecnologia i les dades. En aquest sentit, les administracions públiques tenen un paper un important, no només quant al compliment de la normativa, sinó també com a impulsors de noves estratègies i tendències enfocades en els usuaris, per ajudar en la prevenció i la millora de la qualitat de vida de les persones.

Joana Marí Cardona

Delegada de protecció de dades i responsable de projectes estratègics de l'Autoritat Catalana de Protecció de Dades