

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



Reflexió sobre la importància de l'educació i la sensibilització en el marc de l'alfabetització digital

23-10-2023

L'evolució constant de la tecnologia exerceix un impacte profund en el nostre món, i dona lloc a canvis significatius en múltiples àmbits de la societat. Aquestes transformacions abasten des del sector empresarial fins al camp de l'educació i la sanitat, i afecten qüestions molt diverses, com ara en la manera en què interaccionem i ens comuniquem.

Malgrat els avantatges innegables que les tecnologies disruptives ens brinden, en la mesura que agilitzen i simplifiquen moltes de les tasques diàries de les nostres vides, la velocitat amb què la tecnologia està sent desenvolupada i implantada supera àmpliament la capacitat de moltes persones per assimilar i comprendre, no només l'ús, sinó també les implicacions per a la privacitat i la seguretat de les dades personals.

Aquesta qüestió té una rellevància indiscutible en la societat actual, ja que la tecnologia digital cada vegada és més present en molts aspectes de la nostra vida quotidiana, tant en l'àmbit professional com en el personal. Per tant, en aquest context, és evident la necessitat d'adquirir habilitats digitals, com ara l'ús bàsic d'ordinadors, tauletes i telèfons mòbils, o bé la navegació web, i fins i tot abordar qüestions més complexes, com la comprensió dels riscos en línia.

L'alfabetització digital fa referència a la capacitat d'utilitzar, comprendre i comunicar-se eficaçment mitjançant les tecnologies digitals. En altres paraules, és el procés pel qual es desenvolupen les habilitats i els coneixements essencials per interactuar de manera significativa amb la tecnologia i utilitzar-la per accedir, avaluar, interpretar i compartir la informació.

La Unió Europea, per exemple, no ha estat aliena a la necessitat de dur a terme polítiques d'alfabetització digital, i ha declarat el 2023 l'Any Europeu de les Competències, en el qual s'inclouen les habilitats digitals.

D'acord amb les dades que consten a l'EUROSTAT, el 2022 més de les tres quartes parts de les empreses de la UE van informar de la dificultat de trobar treballadors amb el conjunt d'habilitats adequat, i una quarta part de pimes consideraven que la disponibilitat de personal qualificat i gerents experimentats era el problema més gran amb què es trobaven. I, especialment, pel que fa

a les habilitats digitals, l'índex d'economia i societat digitals (DESI) del 2021 va mostrar que el 44% de les persones a la UE i un terç de la força laboral europea no tenen habilitats digitals bàsiques.

Tenint en compte aquestes dades, la UE vol arribar en l'Any Europeu de les Competències a l'objectiu, almenys, que el 80% dels adults compti amb capacitats digitals bàsiques i que hi hagi 20 milions d'especialistes en TIC a la UE a través de diferents iniciatives, com ara posar a disposició dels estats membres de la UE fons econòmics per finançar reformes relacionades amb les capacitats (com els Next Generation EU i el Mecanisme de Recuperació i Resiliència o el Mecanisme Connectar Europa (CEF)), o bé el llançament de la Plataforma Europea d'Ocupació i Habilitats Digitals per posar a disposició de tothom la informació i els recursos sobre habilitats digitals.

Una altra de les iniciatives de la UE és el Pla d'acció d'educació digital (2021-2027), l'objectiu del qual és contribuir a l'educació digital d'alta qualitat, inclusiva i accessible a Europa a través del foment del desenvolupament d'un ecosistema educatiu digital d'alt rendiment i la millora de les competències i les capacitats digitals per a la transformació digital.

No obstant això, sense minimitzar la rellevància que cal atorgar-li, l'alfabetització digital podria no ser suficient per a la plena comprensió de les implicacions en matèria de privacitat i seguretat de les dades personals que sorgeixen de l'accelerada evolució de les tecnologies disruptives.

Perquè cal tenir en compte que, per exemple, la intel·ligència artificial (IA), l'internet de les coses (IdC), la biotecnologia i els avenços tecnològics, si bé poden resultar molt útils en la vida quotidiana, o en àmbits tan significatius com la salut, el medi ambient o l'educació, alhora obren la porta a noves oportunitats d'ús indegut o la vulneració de dades sensibles. L'aparició de conceptes emergents com l'aprenentatge profund, les xarxes neuronals o l'automatització massiva, introdueix capes addicionals de complexitat que sovint són difícils de desxifrar pel públic en general, fins i tot amb la implementació de polítiques destinades a fomentar l'alfabetització digital de la població.

Però, a més, també cal considerar l'augment de la interconnexió entre dispositius i sistemes mitjançant l'IoT i altres tecnologies disruptives, que crea una xarxa complexa de flux de dades que es comuniquen constantment entre diversos punts, fet que complica la comprensió del procés de captació, emmagatzematge, processament i transmissió de les dades.

Davant d'aquesta complexitat, cal que es promogui l'educació i la sensibilització sobre la tecnologia disruptiva i la seva implicació en la protecció de dades personals. La comprensió sobre aquestes qüestions és fonamental per empoderar les persones per prendre decisions informades sobre la interacció amb les tecnologies digitals, fet que fa augmentar la probabilitat de conèixer com protegir la seva privacitat i prendre mesures per salvaguardar les seves dades davant potencials amenaces.

I és que, a diferència de l'alfabetització digital, la qual té com a objectiu principal capacitar les persones per aprofitar els recursos digitals al seu abast, l'educació i la sensibilització no només es limiten a proporcionar coneixements relatius a la capacitat o competències, sinó que també aspiren a desenvolupar el pensament crític dels usuaris d'aquestes tecnologies. Podríem dir que les persones sensibilitzades no es limiten a adoptar les noves tecnologies sense qüestionar els

riscos potencials que poden implicar, sinó que adquireixen la capacitat d'avaluar-les de manera crítica, ponderant els seus avantatges i riscos en relació amb la seva privacitat i dades personals, abans de fer-ne ús.

D'acord amb el considerant 166 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquests (RGPD), l'objectiu del RGPD és "[...] protegir els drets i les llibertats fonamentals de les persones físiques i, en particular, el seu dret a la protecció de les dades personals, i garantir la lliure circulació de les dades personals a la Unió [...]".

Encara que les disposicions del RGPD, en un sentit estricte, no estiguin orientades específicament a l'educació i la sensibilització de la població en general sobre el tractament de les seves dades personals, és evident que l'obligatorietat dels responsables del tractament de complir determinades disposicions sí que permeten a la població obtenir informació sobre qüestions rellevants que afecten el tractament de les seves dades. Això, juntament amb la sensibilització i educació, facilita l'empoderament i fomenta la capacitat crítica en relació amb els riscos associats a l'ús d'aquestes tecnologies.

Potser la previsió més evident d'aquesta idea es reflecteix en el contingut de l'article 13 del RGPD, el qual estableix la informació que els responsables del tractament han de proporcionar als interessats quan obtinguin dades personals directament d'aquests; o bé l'article 14 del RGPD, quan la informació no provingui directament de l'interessat sinó d'un tercer. Aquestes previsions contribueixen a la consciència dels individus sobre la recopilació i utilització de les seves dades personals, i promociónen la seva participació activa i la capacitat crítica en la seva relació amb les tecnologies i la privacitat de les dades.

Així, la identitat del responsable del tractament, la seva ubicació i la finalitat del tractament són qüestions que, juntament amb l'educació i la sensibilització, doten qualsevol individu de la capacitat de prendre decisions amb prou autonomia. La possibilitat de prendre decisions informades i autònomes proporciona una base fonamental per a la interacció amb les tecnologies, de manera que el seu ús es pot ajustar a les necessitats i preferències individuals.

Sens dubte, un altre mecanisme que contribueix a reforçar l'empoderament de la població en general és el dret d'accés establert a l'article 15 del RGPD. A través d'aquest dret, qualsevol interessat té el dret d'obtenir del responsable del tractament informació relativa al tractament de les seves dades personals. Aquest dret d'autodeterminació informativa permet a l'interessat obtenir informació que li permet comprovar que el responsable del tractament continua sent fidel i transparent respecte a la informació que li va proporcionar en el moment de la captació. Exercir aquest dret reforça la confiança i el control de les persones sobre les seves pròpies dades i la manera en què són utilitzades. Així, aquest mecanisme complementa l'educació, la sensibilització i el pensament crític, i assegura que les persones tinguin un paper actiu en la seva relació amb les tecnologies digitals i la protecció de dades.

Fins i tot, encara que no sigui requisit exercir el dret d'accés, és clar que l'accés a aquesta informació per part d'una persona sensibilitzada, d'acord amb els termes esmentats prèviament, li permet analitzar de manera crítica el tractament de les seves dades personals. I, si ho considera

necessari, pot prendre accions pertinents mitjançant els altres drets reconeguts en el RGPD, com ara la rectificació, la supressió, la limitació o l'oposició al tractament, per tal d'influir en la manera en què les seves dades són gestionades i utilitzades.

Però no es pot obviar que existeix un factor que no depèn únicament de la població en general. Tot i que la població pugui estar prou educada i sensibilitzada sobre les implicacions i els riscos per a la protecció de dades relacionats amb l'ús de determinades tecnologies, també hi intervenen de manera fonamental el responsable del tractament i, per descomptat, les autoritats de control.

D'entrada, l'article 25 del RGPD estableix el principi de la protecció de dades des del disseny i per defecte, el qual implica que els responsables del tractament han de determinar i implementar, en el moment de definir els mitjans del tractament i durant la seva execució, les mesures tècniques i organitzatives adequades per assegurar l'aplicació efectiva dels principis de protecció de dades.

No obstant això, és cert que un dels reptes significatius que es plantegen amb les tecnologies disruptives és la manca de transparència o la reticència, potser per motius comercials, dels responsables del tractament a informar sobre el potencial i l'abast de la seva tecnologia en relació amb el tractament de dades personals. Això pot dificultar la comprensió per part dels usuaris sobre com s'utilitzen les seves dades i quins riscos poden sorgir. En aquests casos, la manca de transparència pot minvar la capacitat de les persones d'exercir control i prendre decisions informades sobre la seva pròpia privacitat i seguretat de dades.

De fet, la manca de transparència pot tenir diferents conseqüències. D'una banda, si no s'han previst polítiques d'educació i sensibilització sobre els riscos associats a l'ús d'una determinada tecnologia en relació amb els drets i llibertats, és probable que la societat sigui més propensa a adoptar aquesta tecnologia si les ofertes són atractives. En aquest escenari, les persones podrien ser menys crítiques a l'hora d'avaluar els riscos i beneficis, i podrien no prendre plena consciència de les implicacions per a la seva privacitat i la seguretat de dades.

D'altra banda, en una societat més conscient dels riscos potencials de les tecnologies, és probable que les persones reaccionin amb un cert escepticisme i exigeixin més transparència i informació als responsables del tractament. En aquest cas, la població podria ser més crítica i estaria disposada a demanar explicacions més detallades sobre com es gestionen les dades personals i quins són els possibles impactes. Tot això, sens perjudici del fet que la manca de transparència pot tenir un impacte significatiu en la reputació del responsable del tractament. Ara bé, aquesta no és una qüestió que tractarem en aquest apunt.

En aquest punt, la intervenció de les autoritats de control es converteix en un element crucial. Entre les seves funcions convé destacar el control de l'aplicació efectiva del RGPD i la seva execució, la promoció de la sensibilització del públic i la seva comprensió dels riscos, normes, garanties i drets en relació amb el tractament, especialment per als infants, i la promoció de la sensibilització dels responsables i encarregats del tractament sobre les obligacions que els incumbeixen en virtut del RGPD (art. 57 del RGPD). Per exemple, podem citar les actuacions dutes a terme per la Commission Nationale de l'Informatique et des Libertés o CNIL (autoritat de control francesa), que van portar a multar Google el 2021 pel fet d'utilitzar galetes publicitàries sense el consentiment adequat i no proporcionar informació clara i completa sobre l'ús de les galetes; o, en la mateixa línia, el mateix any, l'autoritat de control de Luxemburg també va sancionar Amazon en un cas similar.

A més, és rellevant esmentar l'exemple més recent de l'alerta causada per la proliferació de l'ús de l'eina ChatGPT. Aquesta situació va portar el Garante per la protezione dei dati personali (autoritat de control italiana) a bloquejar temporalment l'accés a aquesta eina des del territori italià davant els dubtes dels riscos per a la privacitat dels usuaris que podia implicar l'ús d'aquesta tecnologia, i l'Autoritat Catalana de Protecció de Dades a recomanar no fer ús de l'eina ChatGPT en la prestació de serveis públics quan es tractin dades personals.

Tanmateix, cal assenyalar que, malgrat la possible eficàcia d'aquestes accions des d'un punt de vista administratiu, la seva percepció per part de la població general pot ser diferent. Sovint, aquestes actuacions només tenen com a conseqüència grans titulars sensacionalistes als mitjans de comunicació. Encara que aquests titulars poden alertar momentàniament la població, en realitat poden no tenir un impacte pedagògic efectiu o fins i tot poden alimentar un corrent d'escepticisme constant, fins i tot quan el responsable del tractament ha abordat posteriorment la situació que va donar lloc a la presumpta infracció.

Per aquest motiu, més enllà de la potestat sancionadora de les autoritats de control, la sensibilització sobre els riscos, normes, garanties i drets també té una importància cabdal. Aquesta combinació podria permetre d'entendre millor els motius que han motivat l'acció de les autoritats de control i les mesures correctives adoptades en cada cas i, a més, ajudaria a reduir la desconexió entre la reacció inicial i el resultat final, de manera que proporcionaria a la població una percepció més ajustada i realista dels esdeveniments en qüestió.

En el cas de l'Autoritat Catalana de Protecció de dades, la necessitat de promoure la sensibilització de la població general i dels responsables del tractament, no ha passat inadvertida i, a més de la posada en marxa del projecte "Qui ets? Dades que parlen de tu", s'ha inclòs explícitament la sensibilització com un dels pilars del Pla estratègic 2023-2028, amb l'objectiu d'empoderar les persones, especialment les més vulnerables, sobre la protecció de les dades personals.

En particular, el pilar relatiu a la sensibilització es divideix en quatre línies d'actuació: la privacitat per a infants i joves; la privacitat en l'àmbit sociosanitari; la presència a la societat i la creació d'un observatori de protecció de dades, com a grup d'experts de l'àmbit acadèmic, professional i de la societat civil que impulsi l'ús correcte de les dades a Catalunya.

Amb aquesta exposició, l'objectiu és la reflexió sobre la importància de l'alfabetització digital en el segle XXI, en la mesura que la tecnologia s'ha integrat pràcticament en tots els àmbits de la vida quotidiana. No obstant això, no s'ha d'ignorar que, juntament amb l'alfabetització digital, cal promocionar polítiques de sensibilització envers els riscos per a la privacitat que les noves tecnologies poden portar i alhora el foment d'un esperit crític en la societat. Tot això adquireix una rellevància que va més enllà de les funcions establertes per la normativa de protecció de dades i les atribuïdes a les autoritats de control.

Aquesta reflexió serveix com una crida a l'acció per abordar la dualitat entre el creixent ús de la tecnologia i la necessitat d'entendre i gestionar els riscos relacionats amb la privacitat i la seguretat. L'empoderament dels individus amb habilitats digitals i una comprensió informada dels perills pot ajudar a abordar aquest repte i a garantir una convivència més segura i respectuosa amb la tecnologia en la societat actual. En definitiva, "El coneixement és poder" (Francis Bacon).



Carlos López Martínez

Lletrat de l'Assessoria Jurídica de l'Autoritat Catalana de Protecció de Dades