GUIA INFORMATIVA

Guia de protecció de dades i bones pràctiques en l'entorn digital

Institut Andorrà de les Dones

Agència Andorrana de Protecció de Dades

Amb el suport de l'Agència Nacional de Ciberseguretat d'Andorra i de l'Àrea de Delictes Tecnològics del Servei de Policia d'Andorra.

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Historial de versions

Versió	Data	Detall de la modificació
Versió 1	4 de novembre del 2023	Document original

Índex

1) Introducció

Ens trobem immersos en una revolució digital que ha canviat el nostre dia a dia, transformant la nostra forma d'interactuar, de treballar o inclús de relacionar-nos amb altres persones. Les tecnologies recents, especialment amb l'aparició d'Internet i els dispositius mòbils, han brindat a la societat innumerables avantatges i beneficis. Això ha permès superar barreres geogràfiques, efectuar la majoria d'accions a distància i, fins i tot, dur a terme tasques complexes en molt poc temps.

Però no tot són avantatges i beneficis. Els avanços també obren la porta a una sèrie de males praxis que es poden derivar de l'ús incorrecte de la tecnologia. Cal fer avinent que la tecnologia en si no és dolenta, sinó que tot depèn de l'ús que se'n fa. En aquest sentit, com és evident, aquesta nova era digital també ha portat una sèrie de desafiaments tècnics i jurídics, especialment en qüestions ètiques i de privacitat de protecció de dades personals.

És important prendre consciència que la nostra informació personal té avui dia un valor quantificable i que es converteix en un actiu molt valuós, tant per a empreses i organitzacions com per a ciberdelinqüents. Actualment, la gran quantitat d'informació que es tracta, en combinació amb tecnologies actuals (com la intel·ligència artificial) i el tractament de dades sensibles (com ara les biomètriques o de salut), situen les persones usuàries en una posició de més vulnerabilitat davant una situació d'accés indegut a la informació per part d'un tercer no autoritzat, arran d'un ciberatac, una pèrdua d'informació, una exposició involuntària d'informació o altres casuístiques semblants.

En aquest context d'irrupció abundant de tecnologies, l'auge dels ciberatacs i la recurrència en els usos inadequats de tecnologies actuals, ja siguin per desconeixement o per mala praxi conscient, fan que certs grups de persones en pateixin més les conseqüències. Són, sovint, col·lectius vulnerables de dones, menors, persones grans i LGTBIQ+.

L'Agència Andorrana de Protecció de Dades (APDA) i l'Institut Andorrà de les Dones (IAD), d'acord amb la Llei 06/2022, del 31 de març, per a l'aplicació efectiva del dret a la igualtat de tracte i d'oportunitats i a la no-discriminació entre dones i homes, concretament amb l'article 17, segons el qual les administracions públiques han d'adoptar mesures preventives i reactives per abordar i fer cessar les situacions de discriminació, volen mostrar el seu compromís per garantir l'ús adequat de les tecnologies per part de la ciutadania andorrana. Han pres, doncs, la iniciativa de desenvolupar aquesta Guia per tal de proporcionar informació d'utilitat i de bones pràctiques per fomentar un tractament adequat de la informació garantint la igualtat, la seguretat i la privacitat.

1.1. Objectiu de la guia

Aquesta Guia té com a finalitat principal conscienciar i sensibilitzar la població sobre els riscos associats al tractament de les dades personals, els perills que es deriven de les noves tecnologies i, en especial, l'impacte en determinats col·lectius de la societat.

Així mateix, aquest document proporciona eines i recursos des d'un prisma pràctic i accessible, per tal d'identificar situacions delicades o crítiques que puguin posar en risc la seguretat o la privacitat, i per fer front a les amenaces sobrevingudes per l'ús d'aquestes tecnologies, cada vegada més integrades en la nostra esfera personal i professional.

A banda del que s'ha exposat, amb aquesta Guia es pretén informar la ciutadania sobre la forma d'exercir els drets que la normativa de protecció de dades li atorga. També proporciona a empreses i organitzacions directrius clares sobre la manera de tractar dades personals, en especial quan siguin de grups de persones vulnerables o dades que presentin un grau de sensibilitat superior.

1.2. Importància de la privacitat en l'era digital

La privacitat és un dret fonamental reconegut en la normativa andorrana i l'europea i en gran part dels països d'arreu del món.

El dret a la privacitat i a la protecció de dades ha adquirit una gran importància aquests darrers anys, tal com hem mencionat anteriorment, amb l'evolució d'Internet, l'aparició dels dispositius mòbils, la incorporació de l'Internet de les coses (IoT) o de dispositius intel·ligents a les nostres llars i oficines, i darrerament amb la consolidació de la intel·ligència artificial (IA).

La digitalització porta associada una sèrie de desafiaments tecnològics i jurídics al voltant de la privacitat de les persones usuàries. Algunes de les tecnologies actualment existents permeten tractar molta informació o determinades dades sensibles, i l'ús o la irrupció d'aquestes eines no pot comportar mai una renúncia a la privacitat. Cal acompanyar l'evolució de les tecnologies, promovent-les amb les degudes garanties i respectant sempre els drets fonamentals de la ciutadania.

L'ús de les plataformes i les tecnologies pretén millorar alguns aspectes de la nostra vida personal o professional, però no poden en cap cas implicar una pèrdua de control sobre la nostra informació o facilitar la comissió d'infraccions o delictes.

En l'entorn d'Internet no hi ha impunitat sobre els actes comesos, i les conductes inadequades poden suposar, entre altres coses, conseqüències administratives, civils o, fins i tot, penals.

Cal que la ciutadania prengui consciència del dret a la privacitat, coneixent les normes i les bones pràctiques en l'ús dels dispositius i les plataformes, per tal que es pugui garantir un bon entorn de convivència i harmonia en l'ecosistema digital.

2) Públic objectiu: col·lectius vulnerables

2.1. Ciberassetjament i abús en línia

El ciberassetjament és una modalitat d'assetjament que succeeix en entorns en línia, generalment a través d'algun plataforma o dispositiu connectats a Internet. Es podria definir com un comportament que es repeteix i que busca atemorir, humiliar o fer que s'enfadin altres persones. Per exemple, difondre mentides o publicar fotografies o vídeos íntims d'algú a les xarxes socials. També inclou altres accions com enviar missatges, imatges o vídeos feridors, abusius o amenaçadors a través de plataformes de missatgeria.[1]

Representa una violació greu dels drets i les llibertats d'una persona, i malauradament les situacions de ciberassetjament han crescut substancialment els darrers anys, especialment després de la pandèmia de la covid-19. A banda d'això, la realitat és que no tota la població pateix de la mateixa manera l'augment d'aquestes activitats il·lícites. Segons diversos estudis de l'àmbit europeu, les dones, i en particular les i els menors d'edat, són subjectes implicats en la major part d'aquests casos.

Més enllà de l'augment dels ciberassetjaments arran de la pandèmia, a partir del 2023 hi ha hagut un increment en la sofisticació d'aquests atacs amb la consolidació de la intel·ligència artificial, que ha comportat l'aparició d'informacions falses o *deepfakes* (alterades amb IA), que sovint han resultat ser imatges manipulades (o falsificades) de menors, nues, creades mitjançant algunes plataformes.[2]

[1] Unicef. (2024). *Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quieren saber acerca del ciberacoso.* Disponible a: <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#:~:text=Es%20un%20comportamiento%20que%20se,través%20de%20plataformas%20de%20mensajería>.

[2] Comitè Europeu de Protecció de Dades (CEPD). (2024). Declaració 1/2024 sobre novetats legislatives referents a la proposta de Reglament pel qual s'estableixen normes per prevenir i combatre l'abús sexual infantil. Disponible a: <https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf>

Les víctimes de ciberassetjament sovint experimenten una violació de la seva intimitat o una pèrdua de control sobre les dades pròpies. És important que quan una persona sigui objecte d'alguna d'aquestes circumstàncies i vulgui cursar una denúncia es posi en contacte ràpidament amb el Servei de Policia, a través de l'adreça electrònica policia@policia.ad, o bé mitjançant el formulari existent al web www.policia.ad, per tal de rebre assessorament sobre la situació, interposar la denúncia corresponent —en cas que s'entengui vulnerat el dret a la protecció de dades— i tallar amb celeritat la cadena de transmissió si s'ha difós informació personal que atempta greument contra la intimitat.

És important tenir present que, segons la Llei qualificada de protecció de dades (LQPD), l'APDA només pot actuar quan es tracti d'una vulneració dels drets relatius a la protecció de dades; si es detecten delictes penals, l'expedient queda en suspens i es trasllada a la Policia.

Exemple: soc estudiant i un dia uns companys de classe creen una imatge meva nua mitjançant una app d'intel·ligència artificial, i l'envien a la resta d'alumnes de l'escola. Puc denunciar aquests fets?

Sí. T'has de posar en contacte amb el Servei de Policia perquè ho investigui. En cas que la infracció l'hagin comès persones menors d'edat, la família o els tutors legals poden respondre econòmicament.

2.2. Ciberviolència i violència de gènere digital

La violència de gènere digital és un tipus de violència en entorns en línia que comporta certes dificultats a l'hora de detectar-la per gran part de la societat, però les seves conseqüències tenen un fort impacte psicològic, social i econòmic sobre les persones que la pateixen. A vegades podria ser objecte de ciberassetjament o persecució d'una dona en línia. No obstant això, també ens podem trobar en situacions de violència de gènere digital arran de casos de difusió de contingut personal o íntim d'una dona a través d'Internet, suplantació d'identitat, amenaces a través de plataformes digitals, etc.

Es podria descriure com una extensió de la violència psicològica, emocional o, fins i tot, física per Internet. Cal fer avinent que aquesta mena de violència pot manifestar-se de diverses formes, incloent-hi l'ús maliciós de dades personals per controlar, amenaçar o humiliar algunes dones.

Aquesta violència es pot concretar en situacions amb una greu invasió de la privacitat, danys físics, econòmics o socials de la dona. A Andorra hi ha diversos mecanismes per fer-hi front i, en cas que sigui necessari, donar suport legal i psicològic a les víctimes. Per a casos de violència de gènere, el telèfon del Servei d'Atenció a les Víctimes de Violència de Gènere és el 181; en cas d'agressió física, sexual o de lesions, s'ha de trucar al telèfon del Servei d'Urgències de l'Hospital Nostra Senyora de Meritxell, el 166; i si hi ha vulneració dels drets fonaments, es pot contactar amb el Raonador del Ciutadà, a través del telèfon 810 585.

En el supòsit que una dona, major o menor d'edat, sospiti d'alguna conducta que pogués emmarcar-se dins d'alguna de les circumstàncies descrites, cal que es posi en contacte amb el Servei de Policia a través de l'adreça electrònica policia@policia.ad per tal de rebre l'atenció i el suport corresponents.

Exemple: la meva parella em revisa constantment les xarxes socials i accedeix als meus dispositius sense permís per tal de controlar en tot moment on soc i què faig.

Pots ser víctima d'una situació de violència de gènere digital. És recomanable que, en cas de detectar-ho, canviïs la contrasenya o les credencials d'accés al telèfon mòbil, al portàtil i a les plataformes on detectis els accessos d'una tercera persona.

2.3. Discriminació en línia

La discriminació en línia la pot facilitar l'ús inadequat de les dades personals, com ara perfils generats automàticament que poden portar a decisions esbiaixades o injustes. Aquesta discriminació pot afectar especialment diferents tipus de públics sensibles o vulnerables, com dones, menors, persones grans o LGTBIQ+. A banda d'aquests col·lectius, també existeixen sovint situacions de discriminació que afecten persones amb diversitat funcional, cultures minoritàries o, fins i tot, comeses per qüestions d'ètnia, religió o classe social.

A Internet hi ha una falsa sensació d'anonimat. Les conductes irregulars o que poden conduir a una determinada irregularitat o delicte són legalment perseguibles pel rastre o l'empremta digital a la xarxa. Malgrat que l'actor d'aquestes conductes sovint pretén ocultar la seva identitat, generalment existeixen dades o metadades (com l'adreça IP) que permeten localitzar la persona que executa la infracció.

Per combatre aquesta discriminació, és essencial, entre altres aspectes, que hi hagi transparència en els algoritmes i les pràctiques de recollida de dades, així com mecanismes efectius per a la revisió i l'oposició de decisions automatitzades.

Exemple: detecto una oferta laboral en un portal d'Internet que només va dirigida a un grup de persones d'un sexe determinat.

Podries ser davant d'una situació de discriminació en línia per raó de sexe. És important que comuniquis aquesta situació a l'IAD mitjançant l'adreça electrònica info@iad.ad perquè pugui analitzar el cas.

2.4. Amenaces a la privacitat en xarxes socials i aplicacions mòbils

Les xarxes socials són una eina perfecta per establir llaços duradors amb persones i entitats, tant en l'entorn personal com en el professional. Ara bé, les xarxes socials són també una font significativa de riscos per a la privacitat, que van des de la recollida massiva de dades fins a la vigilància o el seguiment sense consentiment.

Per protegir els usuaris i les usuàries, especialment de grups sensibles, és primordial desenvolupar i promoure configuracions de privacitat *robustes*, polítiques de consentiment clares i eines fàcils d'utilitzar per poder gestionar sense dificultats el grau de visibilitat o exposició que es vol donar al perfil de la xarxa social, i graduar el rang d'accés a la informació personal.

És rellevant que l'usuari o la usuària dediqui uns instants a llegir i entendre exactament les condicions de privacitat del perfil de la xarxa social en el moment d'obrir un compte.[3] També és crucial, especialment al principi, limitar el nombre de dades personals que s'aporten al perfil (és recomanable incorporar-hi tan sols les mínimes i obligatòries per obrir el compte) i ser curós amb el nombre de contactes amb accés al perfil.

[3] Campanya «Protegeix les teves dades, fes prevaldre els teus drets». APDA (2023). Disponible a: <https://www.apda.ad/noticia/internet-no-oblida>.

Exemple: soc usuari/ària de xarxes socials i, conscient que els ciberatacs són molt habituals, vull incorporar-hi mesures de seguretat adequades que evitin un possible accés no autoritzat a la meva informació.

És important la incorporació de contrasenyes *robustes* (que incorporin un mínim de deu caràcters alfanumèrics i almenys algun símbol), i activar la verificació en dos passos, o l'autenticació de doble factor,[4] sempre que sigui possible. També és interessant verificar la configuració d'accés remot (tipus WhatsApp Web) o la configuració de compartició d'informació amb perfils vinculats de l'estil *mode família,* en què a través d'altres dispositius es pot veure el contingut compartit, així com sessions obertes del correu electrònic.

En un món cada cop més connectat, les aplicacions mòbils formen part de la nostra vida quotidiana i faciliten tasques com la comunicació, les compres o la gestió d'informació personal. Tanmateix, poden recollir una gran quantitat de dades sobre els usuaris o les usuàries: des de la ubicació, els contactes, missatges, imatges fins a informació sensible com l'activitat financera o mèdica. És important saber què es comparteix i com controlar aquesta informació per evitar que se'n faci un ús indegut o es vulneri la privadesa.[5]

[4] *Autenticació de doble factor.* Autoritat Catalana de Protecció de Dades. Disponible a: <https://apdcat.gencat.cat/ca/documentacio/dadesticsegures/autenticador-de-doble-factor/>.

[5] *Protegeix la teva privadesa a les aplicacions mòbils.* APDA (2024). Disponible a: <https://www.apda.ad/noticia/protegeix-la-teva-privadesa-a-les-aplicacions-mobils>.


Per què és important protegir la teva privadesa?
Les aplicacions mòbils poden recollir gran quantitat de dades sobre tu: la teva ubicació, contactes, hàbits de navegació, i molt més.
Pren el control de la informació que comparteixes!
apda

3) Configuració inicial de la privacitat

La configuració inicial de la privacitat és un pas fonamental per a qualsevol usuari o usuària que comença a utilitzar dispositius digitals, com ordinadors, telèfons intel·ligents o tauletes, com també quan es registra o es cursa l'alta com a usuari o usuària en serveis en línia, com ara xarxes socials o aplicacions. A continuació es presenten algunes de les principals recomanacions que cal tenir en compte.

3.1. Configuració dels paràmetres de seguretat i privacitat

Xarxes socials: quan configuris els teus comptes o perfils en xarxes socials és essencial revisar i ajustar tant les opcions de privacitat com les de seguretat. Això inclou controlar qui pot veure les teves publicacions, qui pot contactar amb tu i com es pot cercar el teu perfil a Internet. És recomanable, amb caràcter general, desactivar la geolocalització si no és necessària, i mirar de limitar l'accés a les teves fotografies i publicacions (i permetre'n l'accés tan sols als amics o contactes de confiança). També és pertinent revisar periòdicament aquestes configuracions, ja que les polítiques de les plataformes poden canviar.

Més enllà d'això, tingues en compte que la teva imatge, tant una foto com un vídeo, és una dada personal. La difusió d'imatges o vídeos publicats sense permís és quelcom que pot afectar la intimitat.

L'APDA vetlla per l'ús correcte de les xarxes socials i esdevé garant del compliment del dret de supressió[6] de les dades personals, en els termes que estableix la norma.

Publicacions: abans de publicar qualsevol cosa en línia, cal pensar en les conseqüències potencials o el possible impacte sobre terceres persones. Quan es comparteix informació o es difonen dades en plataformes obertes al públic o

[6] Formulari per a l'exercici del dret de supressió. (APDA). Disponible a: <https://www.apda.ad/assets/pdf/models/Model_d_exercici_del_dret_de_supressio.pdf>.

tancades però amb accés a un alt nombre de contactes, resulta aplicable la normativa de protecció de dades.

Evita compartir informació personal i en especial les dades següents: el domicili, números de telèfon, la data de naixement, el número de passaport o el document d'identitat o detalls financers (per exemple, el número de compte). Recorda que la informació a vegades acaba en mans inesperades i més enllà d'això, sovint, un cop publicada, la informació pot ser difícil d'eliminar completament.

Dispositius: tant en dispositius mòbils com en ordinadors, cal habilitar sistemes de bloqueig de pantalla. El bloqueig ha de configurar-se per tal que, després d'un cert període de temps d'inactivitat (per exemple, un o cinc minuts) pugui activar-se sol. També s'ha de tenir en compte la visibilitat de les notificacions quan el dispositiu es troba bloquejat, ja que podria permetre veure codis enviats per l'ús dels dobles factors o bé per donar-se d'alta en serveis.

El patró de bloqueig segur pot ser mitjançant contrasenya o codi de punts, segons com ho permeti cada dispositiu. L'autenticació biomètrica (com la identificació d'empremtes digitals o el reconeixement facial) pot ser una opció segura sempre que el sistema utilitzat presenti garanties suficients. Es pot considerar un sistema adequat el que custodiï la informació biomètrica exclusivament en un àmbit local (per exemple, en el mateix dispositiu), de forma xifrada (sense que es pugui accedir a la dada en text pla, és a dir, un fitxer sense mesures de seguretat i fàcilment accessible a ull nu), i quan la finalitat sigui exclusivament per a qüestions de seguretat, sense observar cap ús secundari o posterior.

Actualitzacions: cal mantenir els dispositius, les aplicacions i els programaris degudament actualitzats. Les actualitzacions sovint inclouen millores de seguretat que protegeixen contra vulnerabilitats i amenaces recents. Activar el sistema d'actualitzacions automàtiques pot resultar una pràctica adequada sempre que sigui possible per assegurar que se'n disposa de l'última versió. Paral·lelament, és aconsellable consultar periòdicament la informació que es

publica al web de l'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD) per tal de conèixer si algun dels dispositius, aplicacions o programaris compten amb alguna vulnerabilitat existent[7] i poder actuar en conseqüència (cessant el tractament o minimitzant-ne l'impacte).

[7] Agència Nacional de Ciberseguretat d'Andorra: <https://www.anc.ad>.

4) Navegació segura

Tant al món real com en el digital hi ha riscos i amenaces que poden afectar els nostres drets i llibertats. Generalment, al món real és més senzill intuir quina situació o context pot desprendre un risc i acostuma a ser més fàcil adoptar algunes cauteles.

En l'entorn en línia, encara que alguns riscos no són tan evidents, és important integrar determinades cauteles que garanteixin una navegació segura, en les interaccions que duem a terme diàriament amb les plataformes d'Internet. Una navegació segura permet que les accions en línia no comprometin la privacitat ni la seguretat. A continuació mostrem algunes bones pràctiques.

4.1. Ús de connexions segures

Quan naveguis per Internet, resulta crucial prestar atenció a les connexions per tal d'assegurar que siguin segures. Quan s'obre una pàgina web o s'accedeix a un portal, és valuós verificar que el lloc web compta amb el protocol HTTPS (Hypertext Transfer Protocol Secure), que generalment es mostra al mateix navegador, en forma de cadenat. El protocol HTTPS ofereix una capa addicional de seguretat, xifrant la informació que s'intercanvia entre el navegador i els llocs web. Aquest xifratge ajuda a protegir les dades personals i evita que un tercer no autoritzat pugui interceptar la informació.

És aconsellable que, per tal de comprovar que s'incorpora correctament aquest protocol, es verifiqui que la URL dels llocs web comenci amb «https://». No obstant això, no s'ha de donar per fet que tot i disposar d'aquest protocol sigui una pàgina legítima, vist que darrerament els ciberdelinqüents també són capaços d'implementar-lo. A banda d'això, quan decideixis connectar-te a una xarxa Wi-Fi pública, és recomanable utilitzar una xarxa virtual (VPN) per impossibilitar qualsevol accés a la informació intercanviada.

4.2. Navegació anònima

La navegació anònima pot ser útil per evitar que es pugui facilitar l'enregistrament d'informació sobre pàgines web, contrasenyes, informació de formularis, web cau o altres dades de llocs web durant la navegació.

La navegació anònima evita que les galetes[8] o altres tecnologies de seguiment (per exemple, píxels o píxels invisibles) que incorporen determinades plataformes o pàgines web es desin al navegador o que el mateix navegador guardi un registre dels llocs web visitats i del contingut que es descarregui l'internauta. Ara bé, és important saber també que la navegació privada o anònima no és efectiva per prevenir el seguiment del nostre dispositiu (mòbil, tauleta, portàtil i ordinador) i sovint pot ocasionar una falsa sensació de privacitat.

Consell: resulta molt recomanable activar la navegació privada quan s'utilitzi un ordinador compartit o es faci ús d'un ordinador des d'un d'accés públic (per exemple, un hotel). En el cas de fer servir un ordinador d'un hotel, si s'activa la navegació d'incògnit, la persona usuària pot accedir al seu compte de correu o perfil de xarxes socials amb la tranquil·litat que les credencials d'accés no es conservaran posteriorment i una altra persona no podrà recuperar la sessió, un cop es tanqui l'ordinador o la pestanya del navegador.

Les finestres de navegació d'incògnit generalment tenen una aparença diferent de les finestres normals. La part superior d'una finestra d'incògnit sol ser gris o blava, depenent del navegador que s'obre. Per obrir una pestanya d'incògnit, cal seguir els passos següents:[9]

[8] *Guia informativa: ús de cookies, política de privadesa i avís legal.* APDA (2024). Disponible a: <https://www.apda.ad/storage/guides/b090S1LGln1k0StXyghFvQ5SeEdVmk3WrCFlfwU6.pdf>.

[9] *Información sobre seguridad tecnológica.* Agencia Española de Protección de Datos (AEPD) (2023). Disponible a: <https://www.aepd.es/areas-de-actuacion/recomendaciones/informacion#:~:text=Haz%20clic%20en%20el%20icono%20de%20menú%20de%20Chrome%20situado,Selecciona%20Nueva%20ventana%20de%20incógnito>.

Internet Explorer

- Opció 1:

A la barra del menú d'Internet Explorer, fes clic a l'opció «Eines». Es desplegarà un menú. A continuació, clica el botó «Nova pestanya *Inprivate*».

- Opció 2:
  Clica el botó secundari a la icona d'Internet de l'Explorer. A continuació, selecciona l'opció de «Començar exploració *Inprivate*».

Firefox

- Opció 1:
  Clica la icona del menú Firefox, situat a la part superior dreta de la finestra del navegador. A continuació, selecciona «Nova finestra d'incògnit».
- Opció 2:
  Sobre l'enllaç, fes clic al botó secundari i tria l'opció «Obrir l'enllaç en una nova finestra privada».

Google Chrome

- Opció 1:
  Fes clic a la icona del menú Chrome situada a la cantonada superior dreta de la finestra del navegador. A continuació, selecciona «Nova finestra d'incògnit».
- Opció 2:
  En un enllaç, fes clic al botó secundari i tria l'opció «Obrir l'enllaç en una nova finestra privada».

Safari

- Opció única:

Fes clic al menú de Safari i selecciona l'opció de «Navegació privada». Confirma «Iniciar la navegació privada».

4.3. Evitar enllaços sospitosos i pesca (*phishing*)

La pesca és una tècnica utilitzada per ciberdelinqüents per obtenir informació confidencial, com ara contrasenyes, números de targetes de crèdit i altra informació de caràcter personal de les seves víctimes. Així mateix, també es fa servir per instal·lar programes maliciosos (*malware*) en els dispositius dels cibernautes.[10]

Els ciberdelinqüents posen en circulació correus electrònics fraudulents que suplanten la identitat d'empreses i organitzacions, principalment, i en els quals, sota qualsevol excusa, sol·liciten a la persona usuària que accedeixi a un enllaç facilitat en el mateix missatge o que descarregui algun fitxer maliciós.

Generalment, els ciberdelinqüents envien a les persones usuàries missatges suplantant la identitat d'una persona de confiança o d'una entitat coneguda per la víctima, com ara el seu banc, una xarxa social, un servei, etc. El *phishing* té per objecte l'engany de l'usuari o a la usuària per tal que la víctima acabi fent alguna acció que comprometi la seguretat o la confidencialitat de les dades.

Els atacs de pesca són cada vegada més sofisticats i poden presentar-se sota l'aparença, cada vegada més real i treballada, de correus electrònics, missatges de text o publicacions de xarxes socials.

Quan es navega a través d'Internet cal extremar les precaucions. Recomanem el següent:

- **Correus electrònics:** no obris correus electrònics, enllaços o fitxers adjunts de remitents desconeguts o que et semblin sospitosos. Para atenció en detalls, com ara errors ortogràfics, adreces de correu electrònic incorrectes o peticions estranyes d'informació personal.

[10] *¿Qué es el phishing?* Instituto Nacional de Ciberseguridad (Incibe) (2021). Disponible a: <https://www.incibe.es/ciudadania/blog/que-es-el-phishing>.

- **Pàgines web:** abans d'introduir informació personal, confidencial o financera en un lloc web, assegura't que l'adreça sigui legítima i estigui xifrada (cerca el símbol d'un cadenat i «https» a la URL).
- **Codis QR:** evita escanejar codis QR que et trobis al carrer o si no confies en la font. Els ciberdelinqüents són capaços de crear un codi QR perquè es descarregui un programari maliciós que infecti el teu dispositiu i sostreure't dades sensibles o dirigir-te a un lloc web fraudulent.
- **Ofertes o descomptes:** compte amb les ofertes que són massa bones o atractives. Quan el preu d'una promoció es troba força per sota del que és el preu de mercat, i el lloc web no és conegut, sospita. Les persones que estafen solen crear llocs falsos de comerç electrònic que desapareixen després de recaptar els diners de les víctimes.

4.4. Eines de bloqueig d'anuncis i publicitat

Un bloquejador d'anuncis i de publicitat té per objecte millorar l'experiència en la navegació de la persona usuària. Bloqueja els anuncis més molestos i desconcertants, com ara les finestres emergents, els bàners i els anuncis en vídeo. A més, evita que es mostrin anuncis a YouTube, Facebook i altres portals de contingut, de manera que cap portal o tercera empresa no pugui interrompre la navegació.

Els bloquejadors d'anuncis també poden reduir la quantitat de dades que les empreses recullen sobre la persona usuària mentre es navega a Internet. A més de proporcionar una millora en la privacitat, aquestes eines poden ajudar que les pàgines es carreguin més de pressa i que millori l'experiència de navegació. No obstant això, és important tenir en compte que alguns llocs web poden requerir que es desactivin aquestes eines per accedir al seu contingut.

Hi ha eines de bloqueig d'anuncis reconegudes per organismes oficials i de renom, com ara l'Institut Nacional de Ciberseguretat d'Espanya (Incibe), que recomanen aplicacions com AdBlock,[11] AdGuard[12] o MyAdChoices.[13]

[11] *AdBlock*. Instituto Nacional de Ciberseguridad (Incibe) (2023). Disponible a: <https://www.incibe.es/ciudadania/herramientas/adblock>.

[12] *AdGuard*. Instituto Nacional de Ciberseguridad (Incibe). (2023). Disponible a: <https://www.incibe.es/ciudadania/herramientas/adguard>.

[13] *MyAdChoices — Transparencia y Control de la Publicidad en Línea.* Agencia Española de Protección de Datos (AEPD) (2018). Disponible a: <https://www.aepd.es/documento/accesit-premio-emilio-aced-2018-myadchoices.pdf>.

5) Protecció de comunicacions

Protegir les comunicacions en línia és crucial per mantenir la confidencialitat i la integritat de la informació personal i les dades intercanviades. Entorn de les comunicacions hi ha diverses mesures que poden aplicar-se i que ajuden a incrementar la protecció.

5.1. Ús de missatges xifrats

El xifratge de les comunicacions és una de les mesures de seguretat àmpliament utilitzades.[14] L'ús de la criptografia és en l'actualitat la manera més eficaç i eficient d'aconseguir la confidencialitat i la integritat de les dades quan es transmeten, sempre que es tingui en compte que hi ha diverses alternatives a l'hora de fer-la servir. A més, segons l'escenari que es vulgui protegir, fer servir una alternativa o una altra pot oferir o no prou garanties per a la protecció adequada de les dades trameses.[15]

Els sistemes de xifratge consten de dos processos:

- **Xifratge:** en aquest procés es transformen les dades (text en pla) en unes dades il·legibles (text xifrat) mitjançant l'aplicació d'una funció matemàtica complexa (algoritme de xifratge) i una clau.
- **Desxifratge:** en aquest procés es transforma el text xifrat en el text en clar mitjançant una segona funció matemàtica complexa i una clau de desxifratge.

[14] *Risk level assessment - Security measures.* European Union Agency for Cybersecurity (ENISA) (ANY). Disponible a: <https://www.enisa.europa.eu/risk-level-tool/help>.

[15] Dictamen en relació amb la consulta formulada per una organització sobre la interpretació de l'article 104 de l'RLOPD i si els sistemes de xifratge que empren l'algoritme de xifratge simètric AES-128 o AES-256 es troben en compliment del marc legal vigent. Autoritat Catalana de Protecció de Dades (APDCAT). (2013). Disponible a: <https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2013/Documents/ca_535.pdf>.

Un factor que cal tenir en compte a l'hora d'escollir el sistema de xifratge és la fortalesa criptogràfica, que és la capacitat del sistema de xifratge de protegir la informació davant d'un atac. Aquesta fortalesa pot dependre de molts factors, però els dos principals són la capacitat que tingui l'atacant d'invertir l'algoritme de xifratge sense conèixer la clau i la dificultat que tingui el mateix atacant de descobrir la clau de desxifratge. En principi, com més llarga sigui la clau de desxifratge, més difícil serà descobrir-la.

A l'hora d'escollir un sistema de xifratge convé assegurar-se que no contingui vulnerabilitats conegudes, sigui perquè s'hagi demostrat que l'algoritme utilitzat no és segur o perquè el temps per calcular totes les claus possibles per desxifrar les dades pugui permetre a un atacant desencriptar les dades sense esforços desproporcionats.

De totes maneres, les mesures de seguretat s'han d'adoptar sempre tenint en compte l'estat de les tecnologies i els riscos als quals estan exposades les dades.

Un sistema de xifratge es pot considerar segur en un determinat moment i deixar de ser-ho un temps després, perquè s'ha descobert una vulnerabilitat o perquè amb l'increment de la potència dels ordinadors el temps de càlcul de les claus de desencriptament s'ha reduït considerablement.

Les principals aplicacions de missatgeria ofereixen un xifratge d'extrem a extrem (per exemple, WhatsApp, Signal o Telegram) i en principi garanteixen que només l'emissor/a i el receptor/a puguin llegir els missatges enviats, ja que la informació és xifrada mentre es transmet (inclús quan passa a través dels servidors de la companyia). Això busca impedir que terceres persones, incloses les de la ciberdelinqüència i fins i tot les operadores dels serveis de missatgeria, accedeixin al contingut de les nostres converses.

5.2. Verificació d'identitat en línia

La verificació d'identitat s'ha d'entendre com un procés mitjançant el qual es pot confirmar que una persona és qui diu ser. Aquest és un aspecte fonamental en la protecció de dades, ja que ajuda a evitar l'accés no autoritzat i, conseqüentment, situacions de frau.

De sistemes de verificació d'identitat n'hi ha de diferents tipus. A continuació en mostrem alguns dels principals:

Mètode	Exemple	Descripció	Avantatges	Desavantatges
Verificació basada en el coneixement	Contrasenya	Introducció d'una contrasenya privada	Fàcil d'implementar	Vulnerable a atacs de força bruta i pesca
Verificació basada en la possessió	Testimoni d'autenticació	Introducció d'un codi temporal generat, generalment a un dispositiu físic	Sol ser més segura que la verificació basada en el coneixement	Resulta un problema si la persona usuària perd el dispositiu de possessió
Verificació biomètrica	Reconeixement facial	Escaneig del rostre de la persona usuària per comparar-lo amb una imatge emmagatzemada	Molt segura	Acostuma a ser més costosa d'implementar i susceptible d'errors (depèn de la dada biomètrica)

Diàriament, entrem a plataformes i entorns d'Internet on se'ns demana un registre o autenticació. Amb caràcter general, procura fer servir contrasenyes *robustes* i utilitzar, sempre que sigui possible, el doble factor d'autenticació.

L'elecció del mètode de verificació d'identitat més adequat dependrà del context i del nivell de seguretat que es necessiti.

5.3. Riscos de compartir informació personal en línia

Actualment, compartir o intercanviar informació personal en línia s'ha convertit en una pràctica quotidiana i en certa manera normalitzada. Les xarxes socials, els fòrums, els blogs i els portals web ens ofereixen una gran quantitat d'espais per connectar i interactuar amb altres persones i entitats, però això pot comportar a vegades un risc per a la privacitat.

A continuació esmentem alguns dels riscos més freqüents:

- **Robatori d'identitat:** els ciberdelinqüents poden fer servir la nostra informació personal per suplantar la nostra identitat i cometre fraus econòmics o delictes en el nostre nom.
- **Accés no autoritzat a les nostres dades:** la informació que compartim pot ser interceptada per terceres persones sense el nostre coneixement o consentiment, cosa que compromet la nostra privacitat.
- **Discriminació:** la informació que compartim pot ser utilitzada per discriminar-nos en els àmbits laboral, social o econòmic. Resulta habitual el plantejament de discriminacions per raó de gènere en algun d'aquests àmbits.

No totes les dades tenen el mateix grau de sensibilitat; és per això que a continuació mostrem una sèrie de categories de dades personals que convindria evitar compartir a les xarxes:

- **Dades economicofinanceres**: números de comptes bancaris, números de targetes de crèdit o dèbit, etc.
- **Dades de salut**: historial mèdic, diagnòstics, medicaments que prens, radiografies, etc.
- **Certes dades identificatives i de contacte**: adreça postal, número de telèfon fix o mòbil, adreça electrònica personal, gènere, número de passaport o d'identitat, data de naixement, país de naixement, etc.

5.4. Consells per protegir la informació de contacte

Si bé a vegades resulta necessari i inevitable compartir certa informació, és important prendre algunes mesures que evitin o minimitzin el risc. Algunes recomanacions són les següents:

1) **Limita l'abast:** no és el mateix compartir informació en una plataforma o perfil obert que en un entorn limitat a un grup concret o definit de persones.
2) **Selecciona les plataformes correctament:** sovint treballem o interactuem amb diferents aplicacions i plataformes. Selecciona bé les plataformes a l'hora de compartir informació. Determinada informació més sensible o privada hauria de compartir-se únicament en les plataformes que ens ofereixen més garanties o més confiança.
3) **Estigues alerta:** mira d'estar alerta per detectar qualsevol anomalia o comportament estrany a la plataforma. Un missatge d'algú desconegut, un enllaç inesperat o la sol·licitud de massa dades per part d'un tercer poden ser conductes que poden desencadenar en una ciberestafa.

6) Supervisió adulta

La supervisió adulta es basa en filtres que permeten establir controls sobre l'ús que fan els infants d'Internet. Són una manera excel·lent d'ajudar a evitar que els i les menors d'edat accedeixin a contingut inadequat en línia.

En general, hi ha tres tipus de controls o supervisió que les persones adultes han de tenir en compte:

- Controls de nivell de xarxa: es configuren al concentrador o rúter (dispositiu de xarxa que s'utilitza per connectar múltiples dispositius en una xarxa local) i s'apliquen a tots els dispositius connectats a aquest concentrador o encaminador (que cobreix tota la llar).
- Controls de nivell del dispositiu: es configuren al mateix dispositiu, com un telèfon intel·ligent, i s'aplicaran independentment de com i on estigui connectat el dispositiu a Internet.
- Controls de l'aplicació: s'estableixen a la plataforma o a l'aplicació. Per exemple, les configuracions aplicades a Google o YouTube.

Hi ha moltes menes de controls disponibles que permeten, per exemple:

- Filtrar i bloquejar el contingut no desitjat que vegin els i les menors, com ara la violència i la pornografia.
- Restringir la informació que es comparteix.
- Establir límits de temps en línia.
- Controlar l'hora del dia que els nens i les nenes poden accedir a Internet.
- Establir diferents perfils perquè cada membre de la família tingui un nivell d'accés adequat.

Protegir els infants dels perills que planteja la tecnologia digital i Internet s'ha convertit en una qüestió essencial.

Afortunadament, hi ha algunes eines excel·lents i avançades disponibles, incloses les app de supervisió adulta, que fan un monitoratge del comportament a la xarxa dels i les menors, i així permeten que els familiars responsables estableixin controls sobre l'activitat d'Internet dels seus infants.

Amb la facilitat d'accés, Internet exposa els i les menors a diverses amenaces, com ara el robatori d'identitat, el ciberassetjament, les estafes a les xarxes socials i el contingut maliciós.

Algunes de les raons per les quals la supervisió adulta a Internet és important en l'era digital són:

- Protegeix els i les menors del contingut inapropiat: el control parental és l'única manera efectiva d'administrar els dispositius digitals dels nens i nenes. D'aquesta manera, es pot restringir l'accés al dispositiu dels i les menors per evitar que tinguin contacte amb contingut inapropiat.
- Permet el bloqueig de llocs web i categories: en molts casos, els pares i mares no poden identificar tots els llocs web inadequats per als seus infants. Aquests llocs web es poden restringir bloquejant totes les categories. Les eines de control parental permeten fer-ho. Per exemple, si es pot bloquejar l'accés a tots els llocs que contenen contingut per a adults, només s'haurà de bloquejar la categoria «Adult».
- Capacitat per combatre el ciberassetjament: els telèfons mòbils i Internet han fet que la infantesa sigui més vulnerable a la intimidació i l'abús a través de les xarxes socials i els missatges de text. Hi ha aplicacions de supervisió adulta que permeten veure els missatges i les trucades entrants i sortints.
- Limitació de descàrregues per mantenir els dispositius segurs: els nens i nenes poden ser fàcilment enganyats i això els converteix en objectius principals per als ciberdelinqüents i els pirates informàtics. És més probable que nens i nenes descarreguin aplicacions i programes que semblen genuïns, però que en realitat són maliciosos i virus. Les dades

personals es poden filtrar i contenir informació confidencial, com ara contrasenyes o informació de comptes bancaris. Els controls parentals permeten limitar les descàrregues de fonts no fiables i sospitoses.

Les principals característiques de les eines de supervisió adulta són:

- Control web: la característica principal d'una eina de supervisió és limitar les pàgines web a què poden accedir els i les menors.
- Accés a aplicacions: impedeix els infants introduir-se en aplicacions determinades, com ara xarxes socials o missatgeria instantània. També es pot evitar que entrin a Google Play o App Store perquè els i les menors no puguin comprar en línia.
- Bloqueig de trucades: si es vol evitar que les criatures truquin o rebin trucades de determinats telèfons, es poden bloquejar. També es poden configurar trucades internacionals o trucades de números desconeguts.
- Alarmes: també és possible configurar alarmes al mòbil de les persones joves per avisar-les de qualsevol cosa.
- Temps d'ús: aquestes eines també permeten portar una supervisió del temps que els infants utilitzen en determinades aplicacions a Internet, com ara jocs o navegadors.
- Geolocalització: amb l'eina de supervisió adulta es pot conèixer el lloc on es troba el o la menor a temps real, i fer-ne un ús responsable estant el menor informat d'aquesta acció i acceptant el control.
- Botó de pànic: en afegir aquesta opció al mòbil del o la menor, es rep un avís en cas de produir-se una situació de perill.

7) Plataformes de cites

L'APDA fa les recomanacions següents per utilitzar les aplicacions de contacte o de cites:

- Descàrrega i registre: abans de descarregar qualsevol aplicació cal comprovar que no és un duplicat fraudulent. L'APDA recomana analitzar el nombre de descàrregues o llegir els comentaris i les valoracions d'altres usuaris o usuàries i estar atents que no es tracti d'un duplicat de la pàgina oficial. A l'hora de crear el compte és important no donar més dades de les necessàries, ja que demanaran el nom, l'edat o l'adreça electrònica. També és important posar una contrasenya *robusta* per evitar que puguin accedir-hi per suplantar la identitat. En cas de crear l'usuari a través del compte d'una altra plataforma, cal recordar que la seguretat del compte que estem creant estarà lligada a la de l'altra. Cal tenir present que l'app pot recopilar informació sobre el comportament, així que s'aconsella llegir detingudament la política de privadesa i els termes i les condicions del servei abans del registre.
- Configuració de privadesa: en la configuració, la majoria de les xarxes socials permeten la possibilitat d'ocultar certa informació o impedir que la mateixa app utilitzi aquestes dades per mostrar possibles parelles. La geolocalització és un altre dels punts crítics d'aquestes aplicacions, ja que mostrar a la resta d'usuaris o usuàries on es troba una persona pot ser un risc. Hi ha dades que són possibles d'amagar. L'APDA recomana deshabilitar sempre la geolocalització quan no s'estigui fent servir l'app.
- Crear el perfil: a l'hora de posar en marxa un perfil, el més habitual és incloure-hi fotografies, nom d'usuari o usuària, gustos, estudis, professió, aficions o fins i tot dades molt més personals. No obstant això, aquesta informació pot fer més vulnerables les persones usuàries. Per això, l'APDA recomana:
    - Utilitzar un nom fictici, sobrenom o només el nom de pila.

  - Ser curosos amb les imatges que s'utilitzen per il·lustrar el perfil, la visibilitat del qual es pot limitar. A través seu, altres persones podrien saber l'adreça postal, el lloc de feina, llocs que se solen freqüentar i, fins i tot, informació més sensible a través de documents que apareguin en un segon pla.
  - Ser discret/a en la publicació de dades, com aficions o gustos.
  - Anar amb compte a l'hora d'incloure enllaços a perfils de xarxes socials o compartir contingut automàticament, com ara fotos d'Instagram, llistes de Spotify, tuits o informació de Facebook.
- Precaució a l'hora de connectar amb altres usuaris o usuàries: en fer «m'agrada» (*match*) amb una altra persona, el més comú és començar una conversa a través de l'aplicació per conèixer-se millor. Cal anar amb compte, ja que és possible que el perfil sigui fals o estigui mentint per aconseguir dades personals.
- Utilitzar altres app de missatgeria: és molt habitual que, després de cert temps parlant a través del xat de l'aplicació, es decideixi intercanviar números de telèfon i parlar per WhatsApp o Telegram. Revisa la informació que mostres als perfils d'aquestes aplicacions i configura els paràmetres de privadesa, com l'hora i la data de l'última connexió o notificacions de recepció i lectura de missatges. També és recomanable no compartir informació personal i evitar l'anomenat sèxting o enviament de fotos o vídeos de contingut sexual.
- Cites: un cop la relació traspassi les pantalles i es decideixi quedar amb l'altra persona, també és important actuar amb cautela:
  - Procura anar acompanyat o acompanyada a la cita i quedar en un lloc públic on hi hagi més gent.
  - Informa algun familiar o persona de confiança dels detalls de la cita.
  - Si puges a un cotxe o accedeixes a un domicili, informa aquesta persona de confiança de la matrícula i l'adreça.

- No et descuidis les claus, el mòbil o documents que continguin informació personal teva i mai no teclegis números secrets a la vista de la teva cita.
- Davant qualsevol situació incòmoda o violenta, no tinguis vergonya de marxar o de demanar ajuda.

8) Drets i recursos legals

La normativa vigent permet dur a terme una sèrie d'accions per fer front a les diverses situacions que succeeixen en el marc d'Internet, i que ocasionen una vulneració de drets i llibertats o que comporten un dany.

Pel que fa a la normativa de protecció de dades, té per objecte permetre a qualsevol persona poder controlar què es fa amb aquestes dades. Això implica saber qui té informació sobre nosaltres, quina és aquesta informació, d'on prové, per a quina finalitat té les dades i a qui les facilita, ja que es tracta d'informació que no pertany a qui la gestiona, sinó al o la titular de les dades o la persona interessada.

6.1. Coneixement i punts en comú del dret a la protecció de dades i el dret a la igualtat

El dret a la protecció de dades és una àrea transversal que es troba plenament alineada amb la defensa d'altres drets fonamentals, com el dret a la igualtat. En aquest sentit, la normativa de protecció de dades té com a finalitat, entre d'altres, reforçar la protecció de dades perquè les dades siguin tractades sempre de forma legítima i equitativa.

La normativa de protecció de dades i, en particular, la Llei qualificada de protecció de dades estableixen una sèrie de principis bàsics que han de regir el tractament de les dades personals per garantir que aquest procediment es faci de manera justa, transparent i amb respecte pels drets individuals.

Aquest principi exigeix que les dades personals no siguin emprades de manera discriminatòria per raó de sexe, gènere, orientació sexual o identitat de gènere. En aquest sentit, la normativa de protecció de dades pretén evitar tractaments inadequats o irregulars que condueixin a situacions discriminatòries, dotant la

ciutadania de la possibilitat de denunciar qualsevol processament que pugui conduir a una situació com les descrites anteriorment.

A continuació esmentem alguns exemples en què la normativa de protecció de dades pot tenir un paper important i garantir situacions d'igualtat:

- **Tractament de dades de les víctimes de violència de gènere:** la normativa de protecció de dades permet evitar que les dades identificatives i de contacte de les víctimes siguin exposades públicament o compartides als mitjans.
- **Processos de selecció de personal:** la protecció de dades permet fer front a situacions de discriminació de gènere en l'àmbit laboral, posem per cas evitant que empreses sol·licitin dades personals excessives o irrellevants per a una posició laboral (per exemple, si una candidata té pensat tenir fills) durant el procés de selecció.
- **Tractament de dades sobre baixes laborals:** la normativa de protecció de dades restringeix molt el tractament de dades de salut en l'àmbit laboral. Si una persona necessita absentar-se per fer alguna prova o revisió mèdica, la normativa de protecció de dades permet que no hagi de donar-ne el motiu exacte o concretar la prova.

6.2. Recursos per a víctimes de ciberassetjament i violència digital

Resulta important detectar i saber reconèixer aviat els signes del ciberassetjament, que poden variar des de missatges amenaçadors i la difusió de rumors fins a la usurpació d'identitat o, fins i tot, la publicació de contingut privat sense consentiment de la persona interessada.

En cas de ser víctima d'una situació de ciberassetjament o violència digital, cal que segueixis els passos següents:

1) **Obtenir proves**

- Desa els missatges o les imatges objecte d'aquesta situació i fes-ne captures de pantalla.
- En determinats casos pot resultar recomanable certificar les captures amb fedataris públics com ara notaris o saigs. Si s'utilitza una empresa especialitzada dedicada a auditories informàtiques, s'encarregarà de certificar continguts o comentaris en línia per poder aportar-los amb totes les garanties en un procés judicial.

2) Contactar amb el responsable de l'autoria del contingut o l'administrador de continguts

- Manifesta per escrit a la persona autora del comentari o mitjà on s'ha publicat que el comentari et resulta molest i tracta d'aconseguir la retirada o l'eliminació del contingut.
- En qualsevol cas, aquesta advertència servirà com a prova en cas de reincidència, ajudarà a confirmar que l'autor o autora ha sigut coneixedor o coneixedora del malestar de la víctima i permetrà que la denúncia pugui prosperar.

3) Contactar amb la xarxa social

- Si la situació s'ha comès en un entorn de xarxa social, denuncia l'acció des de la mateixa xarxa social.
- A banda d'això, bloqueja l'atacant com a mesura addicional.

4) Denunciar davant els cossos de seguretat

- Presenta una denúncia al Servei de Policia en què es descriguin els fets.
- Adjunta a la denúncia les proves dels fets i els correus en què sol·licitaves la retirada de contingut; per això recomanem haver certificat el contingut abans que es pugui eliminar.

5) Presentar una denúncia a l'APDA

- En cas que resulti vulnerat el dret a la protecció de dades, sigui per la publicació de continguts (per exemple, dades personals, fotografies o àudios) sense consentiment o per tractar dades d'una tercera persona sense permís (per exemple, suplantant un perfil de xarxes socials), es pot presentar una denúncia davant l'APDA. Ara bé, si es detecta que es tracta d'un delicte penal, el procés queda suspès i es trasllada a la Policia.

9) Conclusions

En un món cada vegada més digitalitzat, on els reptes tecnològics esdevenen habituals, la protecció de dades i la igualtat són cabdals per construir una societat justa i equitativa. Aquesta Guia posa de manifest la importància de protegir la privacitat i les dades personals, especialment quan resultin de col·lectius sensibles, atès que presenten més vulnerabilitats davant de situacions de discriminació.

L'APDA i l'IAD han treballat conjuntament en aquesta Guia, amb el suport de l'Agència Nacional de Ciberseguretat i l'Àrea de Delictes Tecnològics del Servei de Policia, amb l'objectiu de promoure recomanacions i bones pràctiques per tal de garantir un entorn digital segur, respectuós i inclusiu per a totes i tots.

Resulta necessari encarar aquest repte de forma conjunta i des dels diferents àmbits d'actuació, des de les institucions públiques fins a les empreses privades, passant també per la ciutadania en general, pel que fa a l'ús responsable de les tecnologies.

L'era digital presenta nombrosos beneficis, però també comporta desafiaments que cal abordar de manera transversal per garantir la protecció de dades i la igualtat en l'entorn en línia, tant de les generacions actuals com de les futures.

L'educació i la formació contínua en matèria de privacitat, seguretat digital i drets fonamentals són clau per construir una ciutadania digital responsable i respectuosa.

Finalment, aquesta Guia també té per objecte recordar la importància en l'aplicació i la incorporació de la protecció de dades i la igualtat des del seu disseny i per defecte, que, lluny de ser ambdós elements opcionals o potestatius, esdevenen indispensables per garantir un futur digital adequat, just i equitatiu.

Agència Andorrana de Protecció de Dades (APDA)

C/ Dr. Vilanova, 15-17

Nova seu del Consell General, planta -5

AD500 Andorra la Vella

Principat d'Andorra

+ (376) 808 115

apda@apda.ad

@AndorraDPA

www.apda.ad

Institut Andorrà de les Dones (IAD)

Av. Tarragona, 58

Edifici Les Columnes, local 5

AD500 Andorra la Vella

Principat d'Andorra

+ (376) 760 900

info@iad.ad

www.iad.ad