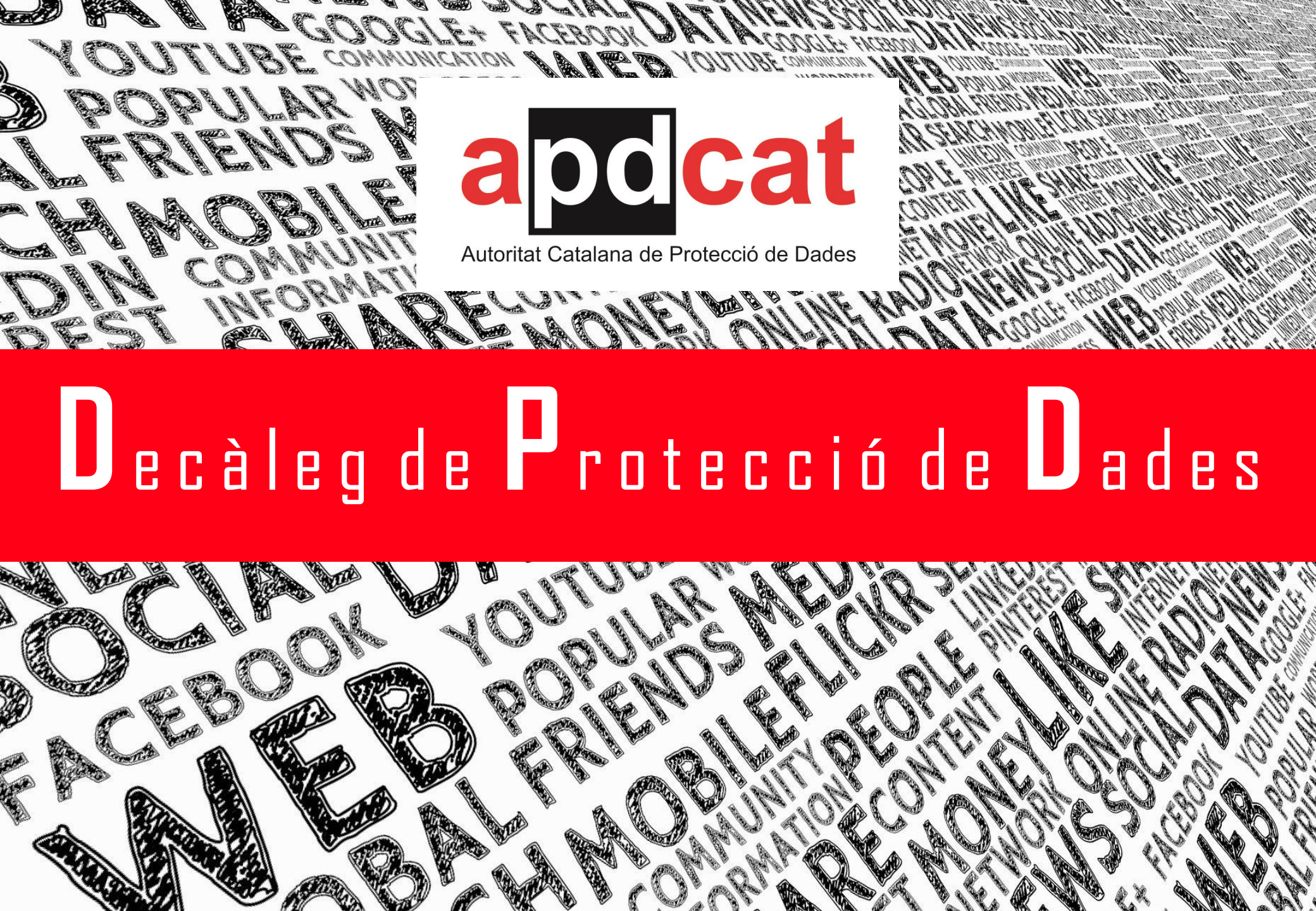

apdcat
Autoritat Catalana de Protecció de Dades
Decàleg de Protecció de Dades

Índex de contingut

1 Menors i Protecció de Dades

2 Dades Mèdiques i Dades Especialment Sensibles

3 Xarxes Socials

4 Intel·ligència Artificial

5 Teletreball

6 Internet de les Coses

7 Dispositius Mòbils

8 Consentiment i Drets de Protecció de Dades

9 Videovigilància

10 Funcions del Delegat/da de Protecció de Dades

Decàleg de Protecció de Dades

apdcat
Autoritat Catalana de Protecció de Dades

Menors i protecció de dades

Internet i les xarxes socials són presents a tots els racons de la societat i els menors no hi són aliens. Els anomenats natius digitals també necessiten formació per fer un ús responsable d'aquestes tecnologies, davant la dificultat per avaluar els riscos, presents i futurs, de fer-ne un mal ús.

apdcat Autoritat Catalana de Protecció de Dades

RGPD

L'RGPD reconeix les dificultats dels menors pel que fa a la protecció de les seves dades. Per això, en fa una especial menció.

El **consentiment** d'un menor només és vàlid si té 14 anys o més. En cas contrari, el consentiment l'han de donar els pares o tutors legals.

Qualsevol **informació** destinada a menors s'ha de presentar d'una manera especialment clara, perquè els menors la puguin entendre.

EDUCACIÓ I CONTROL PARENTAL

Tot i ser natius digitals, els menors necessiten formació per fer un bon ús de la tecnologia: prendre consciència dels riscos de seguretat i dels riscos associats a la publicació de dades personals.

L'**assetjament a través d'internet** és particularment rellevant. Cal que n'estiguin informats. Han de saber reaccionar quan el pateixen o l'observen i, també, evitar caure en aquestes pràctiques.

Les **aplicacions de control parental** poden ajudar els pares a limitar i controlar l'ús de les xarxes. Ara bé, aquesta és una opció sovint qüestionada que no pot substituir l'acompanyament de la familia.

AMENACES

Protegits per una pantalla, és més probable caure en conductes de risc. Cal conèixer les amenaces que afecten els menors més directament:

- Aproximadament un 90% dels adolescents utilitza les xarxes socials, les quals fomenten la **compartició de dades personals**. Cal ser molt curós amb què i amb qui es comparteix una informació. Un cop compartida, és molt difícil recuperar-ne el control.
- El **ciberassetjament** (o *cyberbullying*) és l'assetjament que té lloc en l'entorn virtual. Té diverses manifestacions: missatges amenaçadors, distribució d'informació que pugui perjudicar o avergonyir la víctima, propagació de rumors, suplantació de la identitat.
- En la **ciberseducció de menors** (o *grooming*), un adult busca guanyar-se la confiança d'un menor a través d'internet, amb l'objectiu d'abusar-ne sexualment.

1

DOCUMENTS D'INTERÈS

- APDCAT. Pautes de protecció de dades per als centres educatius
- F. Labrador, A. Requesens i M. Helguera. Guía para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos
- M. Garmendia, C. Garitaonandia, G. Martínez i M. A. Casado. Riesgos y seguridad en internet: Los menores españoles en el contexto europeo
- A Girl Like Her (2015), dirigida per Amy S. Weber
- Trust (2010), dirigida per David Schwimmer

Dades mèdiques i dades especialment sensibles

2

apdcat Autoritat Catalana de Protecció de Dades

L'RGPD qualifica algunes categories de dades com a especialment sensibles; són les categories especials. Aquestes dades poden afectar de forma significativa els drets i les llibertats de les persones i, per això, reben una protecció especial. Entre aquestes, hi ha les dades mèdiques, genètiques i biomètriques utilitzades per identificar persones.

CATEGORIES ESPECIALS

Són dades de categories especials les que revelen:

- Origen ètnic o racial.
- Opinions polítiques.
- Creences religioses o filosòfiques.
- Afiliació sindical.
- Dades genètiques.
- Dades biomètriques amb l'objectiu d'identificar una persona.
- Dades de salut.
- Dades sobre la vida o l'orientació sexual.

Tot i no ser de categories especials, les dades de condemnes i infraccions penals també tenen limitacions en el tractament.

QUAN ES PODEN TRACTAR?

L'RGPD prohibeix que es tractin aquestes dades, llevat que es doni alguna de les condicions de l'art. 9.2. Entre d'altres:

- Consentiment explícit.
- Ocupació, seguretat social i protecció social (d'acord amb la llei).
- Interès vital quan l'interessat no pot donar el consentiment.
- Organitzacions sense ànim de lucre pels seus membres i fins.
- Dades fetes públiques per la persona interessada.
- Formulació, exercici o defensa en reclamacions judicials.
- Interès públic essencial (d'acord amb la llei).
- Salut o atenció social (d'acord amb la llei).
- Salut pública (d'acord amb la llei).
- Arxiu, investigació i estadística (d'acord amb la llei).

QUÈ SÓN LES DADES DE SALUT?

Són les dades relatives a la salut física o mental d'una persona física, inclosa la prestació de serveis d'atenció sanitària.

Això inclou qualsevol número, símbol o dada assignada a una persona física que la identifiqui a efectes sanitaris; la informació obtinguda de proves o exàmens, inclosa la procedent de dades genètiques i mostres biològiques; informació relativa a una malaltia, una discapacitat, la situació de baixa laboral, el risc de patir malalties, l'historial mèdic, el tractament clínic o l'estat fisiològic o biomèdic de la persona interessada.

CONSENTIMENT DEL PACIENT?

No és necessari que un metge o centre mèdic demani el consentiment al pacient per tractar-ne les dades amb finalitat d'assistència sanitària. Sí que cal, però, per a d'altres finalitats; per exemple, per enviar publicitat.

El responsable del tractament sempre s'ha d'informar el pacient sobre el tractament de les seves dades.

APLICACIONS DE WELLNESS

Són aplicacions que fan un seguiment de l'estat físic o de la salut. Recullen una quantitat important de dades de salut (ritme cardíac, calories consumides, exercici realitzat, dieta, etc.).

Cal analitzar la informació de protecció de dades abans de començar a utilitzar-les: responsable, finalitat, comunicació a tercers, etc.

2

DOCUMENTS D'INTERÈS

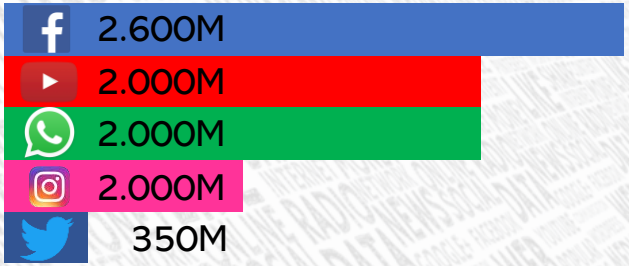
- APDCAT. *Guia de protecció de dades per a pacients i usuaris dels serveis de salut*
- European Patients Forum. The new EU Regulation on the protection of personal data: what does it mean for patients?
- AEPD. *Guía para pacientes y usuarios de la Sanidad*

Xarxes socials

3

Les xarxes socials són la manera de mantenir el contacte amb amics, familiars, companys de feina, etc. Veient el gràfic d'usuaris mensuals, no hi ha dubte que són un instrument d'ús majoritari.

Els dispositius mòbils han donat immediatesa a les xarxes socials: text, veu, fotos, vídeos i geolocalització es comparteixen en el mateix moment de generar les dades.



apdcat
Autoritat Catalana de Protecció de Dades

RISCOS

El principal risc de les xarxes socials rau en la **informació que compartim**. Bé perquè compartim informació inapropiada o bé perquè la compartim amb gent inapropiada. Un cop compartida, és impossible recuperar-ne el control. Les conseqüències poden ser difícils de valorar en el moment de compartir-la i, de fet, es poden materialitzar amb certa posterioritat. Per exemple, és comú que una organització cerqui a les xarxes socials informació sobre candidats a un lloc de treball. La immediatesa que permeten els dispositius mòbils incrementa la probabilitat de les conductes de risc.

El **robatori d'identitat** és produeix quan una altra persona controla de forma no autoritzada un perfil associat a nosaltres. Es pot produir com a conseqüència del robatori de les credencials o perquè l'atacant ha creat un perfil fals amb la nostra informació (*catfishing*).

La **geolocalització** és un servei que incorporen algunes xarxes socials. Per exemple, per contactar amb amics propers. Cal ser molt curosos amb el seu ús: facilita el seguiment de les persones i, fins i tot, pot facilitar un robatori. La web pleaserobme.com mostrava la informació de geolocalització obtinguda de xarxes socials i la relacionava amb l'adreça del domicili.

RECOMANACIONS

Abans de publicar una **informació,** pensa si convé fer-ho:

- No facis comentaris ni publiquis fotos ni vídeos que et puguin perjudicar en el futur.
- No publiquis informació personal, com ara l'adreça, data de naixement, telèfon, etc. Considera la possibilitat d'utilitzar un pseudònim.

Avalua quines **persones** han de poder contactar amb tu i tenir accés a la informació que publiques:

- No acceptis peticions d'accés de persones que no coneixes.
- Abans d'acceptar una petició d'amistat, comprova que la petició la fa qui diu ser.

Protegeix els **dispositius d'accés**. Un ordinador amb les credencials guardades o un dispositiu mòbil és una porta d'accés al nostre perfil.

Respecta la **privacitat dels altres**. No publiquis informació personal d'altres persones sense el seu consentiment. És poc ètic i pot ser delicte.

Utilitza les **opcions de privacitat** disponibles: qui pot contactar amb tu, qui pot veure el teu perfil, qui pot accedir al contingut multimèdia, etc.

Desactiva la **geolocalització,** si no la necessites.

3

DOCUMENTS D'INTERÈS

- CESICAT. Guia per a l'ús segur de les xarxes socials.
- ENISA "Onlie as soon as it happens"

Intel·ligència artificial

4

Avui en dia, l'ús de la intel·ligència artificial (IA) s'ha generalitzat i és comú sentir-ne referències en qualsevol camp. A grans trets, la **intel·ligència artificial** busca donar a les màquines la capacitat de prendre decisions complexes, abans limitades a les persones. També es parla d'**intel·ligència augmentada**, quan es vol remarcar la cooperació entre persones i màquines.

No és una tecnologia nova. El terme *IA* es va començar a utilitzar als anys 50 del segle passat, però ha estat en les dues darreres dècades que l'ús s'ha generalitzat: recomanadors (de notícies, de pel·lícules, etc.), assistents personals (Siri, Alexa, etc.), traducció automatitzada, reconeixement de veu, conducció automatitzada, diagnosi mèdica, etc.

apdcat
Autoritat Catalana de Protecció de Dades

RISCOS

Els riscos depenen en gran mesura de l'aplicació concreta. Aquí ens centrem en els més relacionats amb la protecció de dades.

Els recomanadors són un gran èxit comercial. Mostrant la informació més rellevant al perfil de cada persona, milloren l'experiència, incrementen el consum, etc. Ara bé, una personalització massa intensa condueix a l'anomenat **filtre bombolla**: mostrar a l'usuari només la informació que coincideix amb la seva personalitat i aïllar-lo d'altres realitats.

La capacitat de personalitzar es pot portar un pas més enllà, buscant **manipular** la gent. En les eleccions dels EUA de 2016, Cambridge Analytica va recollir (sense consentiment) informació de més de 80 milions d'electors, per personalitzar el missatge que rebien de Trump segons la seva forma de pensar.

La IA no té prejudicis, però pot **discriminar** igual que ho fan les persones. Els algorismes s'han dissenyat i entrenat en un context social i és probable que en reprodueixin els patrons discriminatoris.

La **precisió** d'un sistema d'IA depèn de molts factors: el model utilitzat, l'entrenament, etc. Un petit percentatge d'errors és inevitable. Això, juntament amb el comportament de **caixa negra,** resta **confiabilitat** a les decisions, cosa especialment problemàtica en aplicacions de fort impacte (per exemple, en diagnosi mèdica).

RECOMANACIONS

Avui en dia, pensar que podem evitar la nostra exposició a la IA és poc versemblant. Per aquesta raó, cal una actitud crítica que ens permeti defensar els nostres drets:

- Cal tenir un **coneixement bàsic** del funcionament de la IA i de les aplicacions en què s'utilitza. L'objectiu és posar en context les decisions i poder jutjar amb criteri si són apropiades.
- **Dret a no ser objecte de decisions automatitzades**. L'RGPD reconeix la variada problemàtica que poden presentar les decisions automatitzades i les prohibeix, si poden tenir un impacte significatiu sobre les persones. Hi ha algunes excepcions però en aquests casos es demanen garanties reforçades; per exemple, el dret a obtenir intervenció humana, a expressar el punt de vista i a impugnar la decisió.
- **Dret a la informació**. No podem exercir els nostres drets sobre les decisions automatitzades si no tenim coneixement del fet. És per això que, si es prenen decisions automatitzades, l'RGPD obliga a informar d'aquest fet i a donar informació sobre la lògica aplicada.

4

DOCUMENTS D'INTERÈS

- APDCAT, *Intel·ligència artificial. Decisions automatitzades a Catalunya*
- University of Helsinki. *Elements of AI,* curs introductori. www.elementsofai.com

Teletreball

5

Si bé el teletreball no és una novetat, amb la COVID-19 ha passat de ser una opció minoritària a ser una necessitat. El teletreball, en si mateix, incrementa els riscos per a la seguretat de la informació, però haver-lo d'adoptar ràpidament i sense planificació prèvia, com ha comportat la COVID-19, els ha magnificat.

Amb el temps, les organitzacions han ajustat els seus sistemes a les necessitats del teletreball (equips portàtils, connexions segures, etc.), però hi ha un punt on les organitzacions no tenen un control total: el seu personal i l'ús que fa dels sistemes d'informació.

AMENACES I RECOMANACIONS

- Treballar en un entorn remot normalitza el respondre a peticions rebudes de forma telemàtica. Els atacants ho aprofiten per fer **atacs d'enginyeria social** (particularment, ***phising***), per exemple demanar credencials o pagaments via correu electrònic. Segons estadístiques, el 50% dels treballadors han patit un atac de *phising* en els darrers 6 mesos i un 10% el pateix cada setmana.

  Unes senzilles pautes poden ajudar-nos evitar molts d'aquests atacs: no donar mai les nostres credencials com a resposta a una petició telemàtica, no seguir enllaços ni descarregar fitxers de correus electrònics no sol·licitats i confirmar les peticions que se surten del procediment habitual. Cal no confiar-se, ja que alguns atacs són difícils de detectar.

- Les dificultats del teletreball a l'hora de desenvolupar certes tasques fa que hi hagi **tendència a esquivar algunes mesures de seguretat** establertes per l'organització.

  Per exemple, segons les estadístiques, el 25% dels treballadors han compartit les seves credencials amb companys. Aquesta pràctica, ja per si mateixa perillosa, ho es més si tenim en compte la tendència a reutilitzar contrasenyes. Compartir una contrasenya amb un company pot facilitar-li accés altres serveis de l'organització o personals als quals no es volia donar accés.

- El tractament de la informació fora de les instal·lacions d'una organització incrementa els **riscos per a la informació**. La informació en format paper és especialment vulnerable, però també ho és la que es guarda en suport digital. Els riscos són variats. Per exemple, treballar en un lloc públic pot posar la informació a l'abast de tercers no autoritzats (escoltar converses, veure la pantalla de l'ordinador, etc.) i mantenir la informació en el dispositiu de teletreball pot comprometre'n la disponibilitat (en cas d'incident).

- L'**ús de dispositius fora de l'organització** incrementa el risc que persones alienes hi tinguin accés. El risc es dona, sobretot, fora del domicili del teletreballador: pèrdua, robatori, etc.

  Cal bloquejar els dispositius quan no s'estan utilitzant, no deixar-los desatesos en llocs públics i ser curós amb les dades sensibles.

- La comunicació és essencial en el teletreball, però l'ús de **xarxes públiques** és perillós. Una xarxa sense xifratge fa que es puguin llegir les nostres comunicacions, un atacant pot crear una xarxa i esperar que la gent s'hi connecti, etc.

- Cal limitar l'ús de les xarxes públiques i, si s'utilitzen, emprar protocols segurs extrem a extrem (VPN, https, etc.). Si això no és possible, cal limitar al màxim la transmissió d'informació sensible.

- Dificultat de l'organització per controlar i fer el manteniment dels equips.

5

DOCUMENTS D'INTERÈS

- AOC. *Guia ràpida per teletreballar amb seguretat*
- Agència de Ciberseguretat de Catalunya. *Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball*

Internet de les coses

6

El terme *internet de les coses, IdC* (en anglès, *Internet of Things, IoT*) fa referència a la interconnexió de dispositius electrònics: electrodomèstics, llums, cotxes, dispositius industrials, dispositius mèdics, etc. Aquesta interconnexió incrementa la funcionalitat. El concepte d'*smart home* i *smart city* té l'IoT com un dels seus pilars. Les aplicacions són molt variades: controlar els dispositius d'una casa a través del mòbil, control del trànsit en temps real, etc.

S'estima que actualment hi ha sobre els 11.000 milions de dispositius IoT i que el 2025 seran uns 21.000 milions. S'espera que l'arribada del 5G sigui un revulsiu per l'IoT.

apdcat Autoritat Catalana de Protecció de Dades

LIMITACIONS I RISCOS

Si bé els riscos de seguretat són una constant en totes les tecnologies, l'IoT té algunes limitacions a l'hora de gestionar-los:

- Dispositius petits i amb bateria que no poden consumir massa recursos en aspectes de seguretat.
- En gran part, dispositius sense sistema de monitorització i amb interacció limitada amb les persones. És difícil detectar canvis de comportament.

Els riscos són molt variats i depenen en gran mesura de l'aplicació concreta. Els classifiquem en dues grans categories:

- **Disrupció o alteració del servei**. El dispositiu no compleix amb la seva funció.
- **Protecció de dades**. Els dispositius recullen, processen i comuniquen informació personal.

L'OWASP dona una llista de **vulnerabilitats comunes** en l'IoT:

- Contrasenyes dèbils o fixades al programari.
- Serveis de xarxa vulnerables al dispositiu IoT.
- Vulnerabilitats als sistemes de control del dispositiu IoT.
- Manca d'un sistema per actualitzar el dispositiu.
- Emmagatzematge i transferència de dades insegura.
- Configuració per defecte insegura.

CAS: MIRAI BOTNET

Una xarxa de zombis (*botnet*) és una xarxa de dispositius que han estat atacats i que ara estan sota el control dels atacants. Els dispositius IoT, pel fet de tenir connexió força permanent a la xarxa, en són objectius potencials. A banda, les limitacions mencionades anteriorment en dificulten la detecció.

El 2016 va aparèixer la xarxa Mirai, que controlava més de 100.000 *routers* domèstics (utilitzant contrasenyes per defecte) i que s'ha utilitzat per fer atacs a gran escala contra grans empreses d'internet. En anys posteriors la *botnet* s'ha diversificat, tant en la manera de prendre el control de nous dispositius com en la tipologia d'atacs (minar bitcoins, etc.). S'estima que actualment té diversos milions de dispositius sota control.

RECOMANACIONS

Per les seves característiques, la tasca de mantenir la seguretat dels dispositius IoT correspon principalment al fabricant. Dit això, els consumidors també hi tenen el seu paper:

- Ser conscients de la necessitat de seguretat en els dispositius IoT i tenir-ho en compte a l'hora d'adquirir-los.
- Seguir les recomanacions del fabricant quant a manteniment i actualitzacions de programari.

6

apdcat Autoritat Catalana de Protecció de Dades

DOCUMENTS D'INTERÈS

- Internet Society. *The Internet of Things: An Overview*
- OWASP. *Internet of Things Top 10*

Dispositius mòbils

7

Els dispositius mòbils han estat una de les tecnologies de més èxit de les darreres dècades. Aquells dispositius que només permetien trucades i SMS són cosa del passat. Ara són petits ordinadors equipats amb tot tipus de sensors (GPS, micròfon, càmera, etc.) i sistemes de comunicació (dades mòbils, WiFi, Bluetooth, NFC, etc.).

L'impacte d'aquests dispositius en la protecció de les dades de les persones és enorme. No només per les seves capacitats, sinó perquè els portem amb nosaltres tot el dia i els utilitzem per a tot tipus de tasques (comunicar-nos amb familiars, amics, etc., navegar per internet, consultar mapes, gestionar l'agenda, fer seguiment de l'activitat física, etc.).

apdcat Autoritat Catalana de Protecció de Dades

RECOMANACIONS

- Utilitza algun sistema per **bloquejar el dispositiu** quan s'està fent servir (contrasenya, patró, etc.). Això dificulta que persones no autoritzades el puguin utilitzar, en cas que hi tinguin accés físic.
- Habilita el **xifratge del dispositiu**. El xifratge protegeix la informació emmagatzemada al dispositiu, de manera que només les persones que en coneixen el codi de desbloqueig hi poden accedir.
- No deixis el **mòbil desatès**. El xifratge i el sistema de bloqueig no garanteixen la seguretat de la informació al 100%. Cal pensar que el dispositiu es desbloqueja repetidament en entorns públics. Per tant, un atacant té opcions reals d'observar el codi de desbloqueig. Fins i tot si no es coneix aquest codi, les notificacions poden revelar informació rellevant.
- Instal·la una **aplicació per esborrar el contingut del mòbil** de forma remota. En cas de pèrdua o robatori, aquest tipus d'aplicacions són l'única opció per esborrar la informació personal.
- Mantingues el **programari actualitzat**. Tenir-lo desactualitzat (tant el sistema operatiu com les aplicacions) és una font de vulnerabilitats i, per tant, una porta d'entrada a atacants.
- **Analitza la seguretat de les aplicacions,** abans d'instal·lar-les. Les aplicacions són el puntal de l'ecosistema dels mòbils, però també són un punt feble en la seva seguretat. Una vulnerabilitat en una aplicació és un punt d'entrada a atacs i hi ha, també, aplicacions malicioses. A banda, moltes aplicacions acostumen a demanar permís per accedir a molta informació que realment no necessiten. Cal, com a mínim, revisar que els permisos que demana una aplicació són raonables.
- Cal tenir **precaució amb l'ús de xarxes WiFi públiques**. Aquestes xarxes que trobem a bars, aeroports, etc. permeten estalviar dades, però porten associats problemes de seguretat. Els atacs són diversos: escoltar comunicacions en xarxes no xifrades o amb protocols de xifratge vulnerables, xarxes creades per un atacant, etc.

7

DOCUMENTS D'INTERÈS

- CESICAT. Guia per protegir i utilitzar de forma segura el mòbil
- CCN. Seguridad en dispositivos móviles (CCN-STIC-450)
- Inteco. Seguridad en dispositives móviles

Consentiment i drets de protecció de dades

El Reglament general de protecció de dades (RGPD) és la regulació normativa europea de protecció de dades actualment en vigor. Un dels objectius de l'RGPD és l'**autodeterminació informativa**; és a dir, donar a les persones un major control sobre la seva informació.

CONSENTIMENT

L'RGPD exigeix que qualsevol tractament tingui una base que el legitimi. N'hi ha diverses i totes són igualment vàlides. Entre d'altres:

- Consentiment informat.
- Interès legítim.
- Obligació legal.
- Interès públic.

Quan la base legitimadora és el consentiment, l'RGPD fixa unes condicions perquè sigui vàlid:

- La petició de consentiment ha de ser fàcilment **distingible** d'altres assumptes i s'ha d'expressar de forma **clara**, utilitzant un llenguatge senzill.
- Cal **informar** l'interessat de la identitat del responsable, de la finalitat del tractament, etc.
- El consentiment és per a un tractament **específic**. Si es demana per a diferents tractaments, cal que es pugui triar un per un a quins es dona consentiment.
- Ha de ser **lliure**. No ha de comportar cap penalització per a l'interessat, més enllà de la impossibilitat de portar a terme el tractament en qüestió. El consentiment no es considera lliure quan hi ha una desigualtat evident entre l'interessat i el responsable del tractament.
- S'ha de poder **retirar** amb la mateixa facilitat amb què s'ha atorgat. Els tractaments duts a terme durant el temps en què ha estat vigent continuen essent vàlids.

DRETS

Dret d'accés. Qualsevol persona té el dret a sol·licitar informació al responsable de tractament sobre si està tractant dades personals seves i, en cas afirmatiu, a rebre diversa informació.

Dret de rectificació. Qualsevol interessat té el dret que es corregeixin les seves dades, si són inexactes o incompletes.

Dret de supressió. Qualsevol interessat té el dret que se suprimeixin les seves dades, quan: ja no són necessàries per a la finalitat per a la qual es van recollir; el tractament es basa en el consentiment i l'interessat l'ha retirat; el tractament es basa en l'interès públic o legítim i s'ha exercit el dret d'oposició; les dades s'han tractat de forma il·lícita.

Dret de portabilitat de dades. L'interessat té dret a sol·licitar les dades personals, si el tractament es fa per mitjans automatitzats i es basa en el consentiment o en el compliment d'un contracte.

Dret de limitació. L'interessat pot sol·licitar que s'aturi el tractament de les seves dades en diversos casos: quan s'ha exercit el dret de rectificació i s'estan verificant les dades, quan s'ha oposat al tractament i s'està verificant si hi ha altres motius que prevalen, etc.

Dret a no ser objecte de decisions automatitzades. Qualsevol interessat té el dret a no ser objecte de decisions basades únicament en un tractament automatitzat, quan aquesta decisió té efectes significatius.

8

apdcat Autoritat Catalana de Protecció de Dades

DOCUMENTS D'INTERÈS

- Reglament general de protecció de dades
- APDCAT. Guia per al compliment del deure d'informar.
- Comissió Europea. RGPD noves oportunitats i noves obligacions.
- Comissió Europea. Son sus datos, ¡tome el control!. Guía para los ciudadanos sobre la protección de datos en la UE

Videovigilància

9

La videovigilància s'utilitza principalment per mantenir la seguretat de persones, bens o instal·lacions. Altres motivacions comunes són el control del personal per part de la seva organització, la prevenció del frau, el control d'operacions, etc. Darrerament, amb la irrupció de la IA, han aparegut gran varietat de noves aplicacions (per exemple, recompte de persones o detecció d'objectes perillosos), algunes de les quals força controvertides (com la identificació automàtica de persones).

apdcat Autoritat Catalana de Protecció de Dades

REGULACIÓ

Llevat dels tractaments de dades en l'àmbit personal o domèstic, la captació d'imatges està regulada per la legislació de protecció de dades.

- Per l'RGPD i l'LODPGDD
- Per la legislació de transposició de la Directiva (UE) 2016/680, en el cas de tractaments fets per les Forces i Cossos de Seguretat en les finalitats que els són pròpies (en procés d'aprovació).

Ens centrarem exclusivament en l'RGPD i la LOPDGDD.

QUÈ ES POT GRAVAR?

La captació d'imatges de la via pública està restringida. Només es poden captar en la mesura que són imprescindibles, amb finalitat de preservar la seguretat de persones, bens o instal·lacions. No es permet, en cap cas, captar imatges de domicilis particulars.

CONSERVACIÓ DE LES IMATGES

Les imatges s'han d'esborrar en un **termini màxim d'un mes** des que es van captar.

Es poden conservar durant més temps, si són necessàries per acreditar la comissió d'actes que atempten contra persones, bens o instal·lacions. En aquest cas, cal posar-les a disposició de les autoritats en un termini màxim de 3 dies.

ACCÉS A LES DADES

El responsable ha de determinar les persones que han de tenir accés a les dades i la finalitat d'aquest accés. S'han d'establir mesures de seguretat per evitar que persones no autoritzades hi accedeixin.

DRET D'INFORMACIÓ

S'ha d'informar que hi ha un sistema de videovigilància. Cal col·locar un **cartell suficientment visible**, com a mínim, als accessos de la zona videovigilada.

Aquest cartell ha d'informar que s'està fent videovigilància, de la identitat del responsable i de com exercir els drets de protecció de dades.

VIDEOPORTERS

Quan l'ús es limita a comprovar la identitat de la persona que truca i a facilitar l'accés a l'habitatge, la normativa de protecció de dades no és d'aplicació. Sí que s'aplica si grava, reprodueix de forma contínua o si el camp de visió és més gran del necessari.

ENTORN LABORAL

D'acord a l'article 89 de la LOPDGDD, una organització pot tractar imatges de càmeres per controlar el personal, segons l'article 20.3 de l'Estatut dels treballadors.

No es poden instal·lar càmeres en espais destinats al descans o lleure dels treballadors, com ara vestidors, menjadors, etc.

DOCUMENTS D'INTERÈS

- APDCAT. *Instrucció 1/2009, de 10 de febrer, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància*
- EDPB. *Guidelines 3/2019 on processing of personal data through video devices*

Funcions del delegat/ada de protecció de dades

10

El delegat de protecció de dades (DPD) és una peça clau en el sistema de protecció de dades que estableix l'RGPD. El DPD supervisa el compliment de l'RGPD dins de la seva organització, de forma independent i sense rebre instruccions. Entre les seves funcions específiques hi ha ser punt de contacte: per a les autoritats de protecció de dades i, també, per als interessats.

apdcat
Autoritat Catalana de Protecció de Dades

QUAN CAL DESIGNAR UN DPD?

És obligatori designar un DPD en els casos següents (veure article 34 de la LOPDGDD):

- Organització o autoritat pública.
- Tractament que comporti l'observació sistemàtica a gran escala.
- Tractament a gran escala de categories especials de dades o de dades relatives a condemnes o infraccions penals.

Per exemple, han de designar DPD les escoles, els hospitals, les empreses de seguretat privada, etc.

Una organització por nomenar un DPD encara que no hi estigui obligada.

POSICIÓ DEL DPD

El responsable del tractament s'ha d'assegurar que el DPD està al cas de tots els assumptes relacionats amb la protecció de dades.

El responsable del tractament ha de donar al DPD el suport necessari en el desenvolupament de les seves tasques i ha d'evitar donar-li instruccions.

FUNCIONS DEL DPD

- Supervisar que l'organització compleix l'RGPD.
- Informar i assessorar el responsable del tractament sobre les seves obligacions de protecció de dades.
- Cooperar i exercir de punt de contacte amb l'autoritat de protecció de dades competent.

PUNT DE CONTACTE

A banda d'exercir de punt de contacte de l'organització amb l'autoritat de control en totes les qüestions relacionades amb la protecció de dades, el DPD també fa de punt de contacte amb les persones interessades.

Els **interessats poden contactar amb el DPD** per qualsevol qüestió relacionada amb el tractament de les seves dades o amb l'exercici dels drets que reconeix l'RGPD.

CONSULTA DE DPD

Les autoritats de control mantenen la llista dels DPD que han estat nomenats per les organitzacions:

APDCAT. Consulta de delegats de protecció de dades

AEPD. Consulta DPD

10

DOCUMENTS D'INTERÈS

- Reglament general de protecció de dades (RGPD)
- Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals (LOPDGDD)
- Grup de treball de l'article 29. *Directrices sobre los delegados de protección de datos (DPD)*
- APDCAT. Consulta de delegats de protecció de dades
  url: https://apdcat.gencat.cat/ca/drets_i_obligacions/responsables/obligacions/delegat-proteccio-dades/consulta-dpd/index.html
- AEPD. Consulta DPD
  url: https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf


apdcat
Autoritat Catalana de Protecció de Dades